

A REAL NULLSTELLENSATZ FOR MATRICES OF NON-COMMUTATIVE POLYNOMIALS

CHRISTOPHER S. NELSON

ABSTRACT. This article extends the classical Real Nullstellensatz to matrices of polynomials in a free $*$ -algebra $\mathbb{R}\langle x, x^* \rangle$ with $x = (x_1, \dots, x_n)$. This result is a generalization of a result of Cimpric, Helton, McCullough, and the author.

In the free left $\mathbb{R}\langle x, x^* \rangle$ -module $\mathbb{R}^{1 \times \ell}\langle x, x^* \rangle$ we introduce notions of the (noncommutative) zero set of a left $\mathbb{R}\langle x, x^* \rangle$ -submodule and of a real left $\mathbb{R}\langle x, x^* \rangle$ -submodule. We prove that every element from $\mathbb{R}^{1 \times \ell}\langle x, x^* \rangle$ whose zero set contains the intersection of zero sets of elements from a finite subset $S \subseteq \mathbb{R}^{1 \times \ell}\langle x, x^* \rangle$ belongs to the smallest real left $\mathbb{R}\langle x, x^* \rangle$ -submodule containing S . Using this, we derive a nullstellensatz for matrices of polynomials in $\mathbb{R}\langle x, x^* \rangle$.

The other main contribution of this article is an efficient, implementable algorithm which for every finite subset $S \subseteq \mathbb{R}^{1 \times \ell}\langle x, x^* \rangle$ computes the smallest real left $\mathbb{R}\langle x, x^* \rangle$ -submodule containing S . This algorithm terminates in a finite number of steps. By taking advantage of the rigid structure of $\mathbb{R}\langle x, x^* \rangle$, the algorithm presented here is an improvement upon the previously known algorithm for $\mathbb{R}\langle x, x^* \rangle$.

1991 *Mathematics Subject Classification.* 16W10, 16S10, 16Z05, 14P99, 14A22, 47Lxx, 13J30.

Key words and phrases. noncommutative real algebraic geometry, algebras with involution, free algebras, matrix polynomials, symbolic computation.

1. INTRODUCTION

This article establishes a non-commutative analog of the classical real Nullstellensatz. The results of Krivine [20], [21], Dubois [9], and Risler [28] established a real nullstellensatz in classical (commutative) real algebraic geometry. For a modern survey of real algebraic geometry (RAG), see the survey by Scheiderer [29] the book of Marshall [26], and the book of Bochnak, Coste and Roy [1].

The main aim of this paper is to extend the real nullstellensatz to non-commutative algebras, in particular free algebras. The earliest such result was proved by George Bergman in an algebra without involution, settling a conjecture of Helton and McCullough [14]. Unfortunately, in an algebra with involution, [14] contains a counterexample to extending Bergman's result. In [16] a major case is settled in a free $*$ -algebra, but much remained open.

A main thrust of real algebraic geometry, in addition to the nullstellensatz, is the positivstellensatz. This holds as well for non-commutative algebras, and is an active area of research dating back to ideas of Putinar [27] and Helton and McCullough [14]. There is a convex branch of that subject, see [15], [12], and [19], and this article feeds into that thereby underlying the sequel [13] to this paper.

This introduction is arranged as follows: in § 1.1 some basic notation will be introduced; in § 1.2 we will discuss the commutative inspiration for the non-commutative nullstellensatz; in § 1.3 we will lay out basic definitions for non-commutative polynomials; in § 1.4 we discuss non-commutative analogs of zero sets and radicals; the main results of the article are then presented in § 1.5; and finally an outline of the article is given in § 1.6.

Our approach to Noncommutative Real Algebraic Geometry is motivated by [16]; for alternative approaches see [30] and [24].

1.1. Notation. Given positive integers ν and ℓ , let $\mathbb{R}^{\nu \times \ell}$ denote the space of $\nu \times \ell$ real matrices. Let $E_{ij} \in \mathbb{R}^{\nu \times \ell}$ denote the matrix with a 1 as the ij^{th} entry and a 0 for all other entries. Let $e_j \in \mathbb{R}^{1 \times \ell}$ denote the row vector with 1 as the j^{th} entry and a 0 as all other entries. Let $1_\nu \in \mathbb{R}^{\nu \times \nu}$ denote the $\nu \times \nu$ identity matrix. Let $A^* \in \mathbb{R}^{\ell \times \nu}$ denote the transpose of a matrix $A \in \mathbb{R}^{\nu \times \ell}$. Let $\mathbb{S}^k \subseteq \mathbb{R}^{k \times k}$ denote the space of real symmetric $k \times k$ matrices.

Although our notation does not correspond to them, one who wishes a general orientation to non-commutative algebras can see Goodearl [10], and for free algebras see P. M. Cohn [6].

1.2. Commutative Inspiration. If I is an ideal in the set of commutative polynomials $\mathbb{R}[x]$ with real coefficients, we say I is **real** if whenever there are some polynomials $p_i \in \mathbb{R}[x]$ which satisfy

$$\sum_i^{\text{finite}} p_i^2 \in I$$

then each $p_i \in I$. The real Nullstellensatz [9], [28] states that if $q \in \mathbb{R}[x]$, then $q(a) = 0$ for all tuples of real scalars a such that $p(a) = 0$ for each $p \in I$ if and only if q is in the **real radical of I** , that is, the smallest real ideal containing I .

A more recent result of Cimprič [3] extends this result to matrices of commutative polynomials. A left submodule I of the free $\mathbb{R}[x]$ -module $\mathbb{R}[x]^{1 \times \ell}$ is **real** if whenever $p_i \in \mathbb{R}[x]^{1 \times \ell}$ satisfy

$$\sum_i^{\text{finite}} p_i \otimes p_i \in \mathbb{R}[x]^{\ell \times 1} \otimes I + I \otimes \mathbb{R}[x]^{1 \times \ell}$$

then each $p_i \in I$. On $\mathbb{R}[x]^{1 \times \ell}$, Cimprič's result states that if $q \in \mathbb{R}[x]^{1 \times \ell}$, then $q(a) = 0$ for all tuples of real scalars a such that $p(a) = 0$ for each $p \in I$ if and only if q is in the **real radical of I** , that is, the smallest real left submodule containing I .

1.3. Non-Commutative Polynomials. We now turn our attention to the space of non-commutative polynomials.

Let $\langle x, x^* \rangle$ denote the monoid freely generated by $x = (x_1, \dots, x_g)$ and $x^* = (x_1^*, \dots, x_g^*)$ —that is, $\langle x, x^* \rangle$ consists of words in the $2g$ free letters $x_1, \dots, x_g, x_1^*, \dots, x_g^*$, including the empty word \emptyset , which plays the role of the identity 1. Let $\mathbb{R}\langle x, x^* \rangle$ denote the \mathbb{R} -algebra freely generated by $\langle x, x^* \rangle$, i.e., the elements of $\mathbb{R}\langle x, x^* \rangle$ are polynomials in the non-commuting variables $\langle x, x^* \rangle$ with coefficients in \mathbb{R} . Call elements of $\mathbb{R}\langle x, x^* \rangle$ **non-commutative** or **NC** polynomials.

The **involution** on $\mathbb{R}\langle x, x^* \rangle$ is defined linearly so that $(x_i^*)^* = x_i$ for each variable x_i and $(pq)^* = q^*p^*$ for each $p, q \in \mathbb{R}\langle x, x^* \rangle$. For example,

$$(x_1x_2x_3 + 2x_3^*x_1 - x_3)^* = x_3^*x_2^*x_1^* + 2x_1^*x_3 - x_3^*$$

1.3.1. Evaluation of NC Polynomials. NC polynomials can be evaluated at a tuple of matrices in a natural way. Let $X = (X_1, \dots, X_g) \in (\mathbb{R}^{n \times n})^g$. Given $p \in \mathbb{R}\langle x, x^* \rangle$, let $p(X)$ denote the matrix defined by replacing each x_i in p with X_i , each x_i^* in p with X_i^* , and replacing the empty word with 1_n . Note that $p^*(X) = p(X)^*$ for all $p \in \mathbb{R}\langle x, x^* \rangle$.

For example, if

$$p(x) = x_1^2 - 2x_1x_2^* - 3, \quad X_1 = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \quad \text{and} \quad X_2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

then

$$\begin{aligned} p(X) &= X_1^2 - 2X_1X_2^* - 3(1_2) \\ &= \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} - 2 \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} - \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 6 & 12 \\ 18 & 21 \end{pmatrix} \end{aligned}$$

1.3.2. Matrices of NC Polynomials. The space of $\nu \times \ell$ matrices with entries in $\mathbb{R}\langle x, x^* \rangle$ will be denoted as $\mathbb{R}^{\nu \times \ell}\langle x, x^* \rangle$. Each $p \in \mathbb{R}^{\nu \times \ell}\langle x, x^* \rangle$ can be expressed as

$$p = \sum_{w \in \langle x, x^* \rangle} A_w \otimes w \in \mathbb{R}^{\nu \times \ell} \otimes \mathbb{R}\langle x, x^* \rangle.$$

Given a tuple X of real $n \times n$ matrices, let $p(X)$ denote

$$p(X) = \sum_{w \in \langle x, x^* \rangle} A_w \otimes w(X) \in \mathbb{R}^{\nu n \times \ell n}$$

where \otimes denotes the Kronecker product. The involution on $\mathbb{R}^{\nu \times \ell}\langle x, x^* \rangle$ is given by

$$p^* = \left(\sum_{w \in \langle x, x^* \rangle} A_w \otimes w \right)^* = \sum_{w \in \langle x, x^* \rangle} A_w^* \otimes w^* \in \mathbb{R}^{\ell \times \nu}\langle x, x^* \rangle.$$

Note that $p^*(X) = p(X)^*$ for any tuple X . If $p \in \mathbb{R}^{\nu \times \nu}\langle x, x^* \rangle$, we say p is **symmetric** if $p = p^*$.

1.3.3. Degree of NC Polynomials. Let $|w|$ denote the **length** of a word $w \in \langle x, x^* \rangle$. A **monomial** in $\mathbb{R}^{\nu \times \ell}\langle x, x^* \rangle$ is a polynomial of the form $E_{ij} \otimes m$, where $m \in \langle x, x^* \rangle$. Let $\mathcal{M}^{\nu \times \ell}$ denote the set of monomials in $\mathbb{R}^{\nu \times \ell}\langle x, x^* \rangle$. The **length** or **degree** of a monomial $E_{ij} \otimes m$ is $|E_{ij} \otimes m| := |m|$.

If p is a NC polynomial, define the degree of p , denoted $\deg(p)$, to be the largest degree of any monomial appearing in p . A NC polynomial p is **homogeneous of degree d** if every monomial appearing in p has degree d . If W is a subspace of $\mathbb{R}^{\nu \times \ell}\langle x, x^* \rangle$, define W_d to be the space spanned by all elements of W with degree at most d .

1.3.4. *Operations on Sets.* If $A, B \subseteq \mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle$, then define $A + B$ to be

$$A + B := \{a + b \mid a \in A, b \in B\} \subseteq \mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle.$$

In the case that $A \cap B = \{0\}$, we also denote $A + B$ as $A \oplus B$; the expression $A \oplus B$ always asserts that $A \cap B = \{0\}$. If $A \subseteq \mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle$ and $B \subseteq \mathbb{R}^{\ell \times \rho} \langle x, x^* \rangle$, let AB be

$$AB := \text{Span}(\{ab \mid a \in A, b \in B\}) \subseteq \mathbb{R}^{\nu \times \rho} \langle x, x^* \rangle.$$

If $A \subseteq \mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle$, let

$$A^* := \{a^* \mid a \in A\} \subseteq \mathbb{R}^{\ell \times \nu} \langle x, x^* \rangle.$$

If $A \subseteq \mathbb{R}^{\nu \times \ell}$ and $B \subseteq \mathbb{R} \langle x, x^* \rangle$, then $A \otimes B$ is

$$A \otimes B := \text{Span}(\{a \otimes b \mid a \in A, b \in B\}).$$

If $p \in \mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle$, then expressions of the form $p + A$, pB , Cp , $D \otimes p$, where A , B , C , and D , are sets, denote $\{p\} + A$, $\{p\}B$, $C\{p\}$, and $D \otimes \{p\}$ respectively.

1.4. **Left $\mathbb{R} \langle x, x^* \rangle$ -Modules.** For $\mathbb{R} \langle x, x^* \rangle$, there is a “Non-Commutative Left Real Nullstellensatz”. Let $p_1, \dots, p_k, q \in \mathbb{R} \langle x, x^* \rangle$. If $q(X)v = 0$ for every $(X, v) \in \bigcup_{n \in \mathbb{N}} (\mathbb{R}^{n \times n})^g \times \mathbb{R}^n$ such that $p_1(X)v = \dots = p_k(X)v = 0$, then q is an element of the “real radical” of the left ideal generated by p_1, \dots, p_k [5]. To generalize this result to $\mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle$, we now generalize the notion of left ideal and real left ideal to non-square matrices of NC polynomials.

The space $\mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ is a free left $\mathbb{R} \langle x, x^* \rangle$ -module. That is, if $q \in \mathbb{R} \langle x, x^* \rangle$, $A \in \mathbb{R}^{1 \times \ell}$ and $r \in \mathbb{R} \langle x, x^* \rangle$, then

$$q \cdot (A \otimes r) := (1_\nu \otimes q)(A \otimes r) = A \otimes qr.$$

In the sequel, we will simplify notation by identifying q with $1_\nu \otimes q$ and simply writing $q(A \otimes r)$ when we mean $q \cdot (A \otimes r)$. We will also simplify our terminology by referring to left $\mathbb{R} \langle x, x^* \rangle$ -submodules $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ as **left modules**.

1.4.1. *Real Left Modules.* Let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a left module. We say that I is **real** if whenever

$$\sum_i^{\text{finite}} p_i^* p_i \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}$$

for some $p_i \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$, then each $p_i \in I$. Note that $\mathbb{R}^{\ell \times 1} I$ is the subspace of $\ell \times \ell$ matrices whose rows are elements of I , and $(\mathbb{R}^{\ell \times 1} I)^* = I^* \mathbb{R}^{1 \times \ell}$ is the subspace of $\ell \times \ell$ matrices whose columns are elements of I^* .

The following result shows that defining a real left module in terms of only $1 \times \ell$ matrices actually covers $\nu \times \ell$ matrices for any dimension ν .

Proposition 1.1. *A left module $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ is real if and only if whenever*

$$(1.1) \quad \sum_i^{\text{finite}} p_i^* p_i \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell},$$

for some $p_i \in \mathbb{R}^{\nu_i \times \ell} \langle x, x^* \rangle$ and some $\nu_i \in \mathbb{N}$, then each $p_i \in \mathbb{R}^{\nu_i \times 1} I$.

Proof. One direction is clear. For the converse, suppose I is real, and suppose that (1.1) holds for some polynomials $p_i \in \mathbb{R}^{\nu_i \times \ell} \langle x, x^* \rangle$. For each p_i ,

$$p_i^* p_i = p_i^* 1_{\nu_i} p_i = \sum_{j=1}^{\nu_i} p_i^* E_{jj} p_i = \sum_{j=1}^{\nu_i} (e_j^* p_i)^* (e_j^* p_i),$$

so that

$$\sum_i^{\text{finite}} p_i^* p_i = \sum_i^{\text{finite}} \sum_{j=1}^{\nu_i} (e_j^* p_i)^* (e_j^* p_i) \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}.$$

Since I is real, each $e_j^* p_i \in I$. Therefore, for each i ,

$$p_i = 1_{\nu_i} p_i = \sum_{j=1}^{\nu_i} e_j e_j^* p_i \in \mathbb{R}^{\nu_i \times 1} I.$$

□

1.4.2. *The Real Radical.* An intersection of real left modules is itself a real left module. Define the **real radical** of a left module $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ to be

$$\sqrt[\text{r}]{I} = \bigcap_{\substack{J \supseteq I, \\ J \text{ real}}} J = \text{the smallest real left module containing } I.$$

1.4.3. *Zero Sets of Left $\mathbb{R} \langle x, x^* \rangle$ -Modules.* If $S \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$, for each $n \in \mathbb{N}$, define $V(S)^{(n)}$ to be

$$V(S)^{(n)} := \{(X, v) \in (\mathbb{R}^{n \times n})^g \times \mathbb{R}^{\ell n} \mid p(X)v = 0 \text{ for every } p \in S\},$$

and define $V(S)$ to be

$$V(S) := \bigcup_{n \in \mathbb{N}} V(S)^{(n)}.$$

If $V \subseteq \bigcup_{n \in \mathbb{N}} (\mathbb{R}^{n \times n})^g \times \mathbb{R}^{\ell n}$, define $\mathcal{I}(V)$ to be

$$\mathcal{I}(V) := \{p \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle \mid p(X)v = 0 \text{ for every } (X, v) \in V\}.$$

The set $\mathcal{I}(V) \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ is clearly a left module. If $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ is a left module, define the **(vanishing) radical** of I to be

$$\sqrt{I} := \mathcal{I}(V(I)).$$

We say a left module is **radical** if it is equal to its vanishing radical.

Proposition 1.2. *Let $V \subseteq \bigcup_{n \in \mathbb{N}} (\mathbb{R}^{n \times n})^g \times \mathbb{R}^{\ell n}$. The space $\mathcal{I}(V) \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ is a real left module.*

Proof. Suppose

$$\sum_i^{\text{finite}} p_i^* p_i \in \mathbb{R}^{\ell \times 1} \mathcal{I}(V) + \mathcal{I}(V)^* \mathbb{R}^{1 \times \ell},$$

where each $p_i \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$. For each $(X, v) \in V$, we have

$$\sum_i^{\text{finite}} p_i(X)^* p_i(X)v = 0 \implies \sum_i^{\text{finite}} v^* p_i(X)^* p_i(X)v = 0.$$

Therefore each $p_i(X)v = 0$, which implies that each $p_i \in \mathcal{I}(V)$. \square

Proposition 1.2 implies that for each left module $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$,

$$I \subseteq \sqrt[r]{I} \subseteq \sqrt{I}.$$

1.5. Main Results. Here is the main result of this article, which is a generalization of [5, Theorem 1.6] to the matrix case.

Theorem 1.3. *Let p_1, \dots, p_k be such that each $p_i \in \mathbb{R}^{\nu_i \times \ell} \langle x, x^* \rangle$ for some $\nu_i \in \mathbb{N}$. Define*

$$J_\nu := \mathbb{R}^{\nu \times 1} \sqrt[r]{\sum_{i=1}^k \mathbb{R}^{1 \times \nu_i} \langle x, x^* \rangle p_i}$$

for $\nu \in \mathbb{N}$. Let $q \in \mathbb{R}^{\nu \times \ell} \langle x, x^ \rangle$. Then $q(X)v = 0$ for all $(X, v) \in \bigcup_{n \in \mathbb{N}} (\mathbb{R}^{n \times n})^g \times \mathbb{R}^{\ell n}$ such that $p_1(X)v, \dots, p_k(X)v = 0$ if and only if $q \in J_\nu$.*

Consequently, if the left module

$$(1.2) \quad \sum_{i=1}^k \mathbb{R}^{1 \times \nu_i} \langle x, x^* \rangle p_i$$

is real, and if $q(X)v = 0$ whenever $p_1(X)v, \dots, p_k(X)v = 0$, then q is of the form

$$q = r_1 p_1 + \dots + r_k p_k,$$

where each $r_i \in \mathbb{R}^{\nu \times \nu_i} \langle x, x^* \rangle$.

This is proven in § 5.3. An interesting corollary is Corollary 6.3, which gives the analog of this Theorem for \mathbb{C} and \mathbb{H} . This Corollary follows from the observation (plus some technical details) that \mathbb{C} and \mathbb{H} can be viewed as subspaces of $\mathbb{R}^{2 \times 2}$ and $\mathbb{R}^{4 \times 4}$ respectively.

In § 9.1 we will present an algorithm for computing $\sqrt[\text{r}]{I}$ for a finitely-generated left module $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$. This algorithm is a generalization of and an improvement upon the Real Algorithm given in [5]. The following theorem, proven in § 9.1.1, states some of its appealing properties.

Theorem 1.4. *Let I be the left module generated by $\iota_1, \dots, \iota_\mu \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$. The following are true for applying the algorithm described in §9.1 to $\iota_1, \dots, \iota_\mu$.*

- (1) *If $\deg(\iota_1), \dots, \deg(\iota_\mu) \leq d$, the polynomials involved in the algorithm all have degree less than $2d$.*
- (2) *The algorithm is guaranteed to terminate in a finite number of steps.*
- (3) *When the algorithm terminates, it outputs a reduced left Gröbner basis for $\sqrt[\text{r}]{I}$.*

1.6. Reader's Guide. Sections 2, 3, and 4 are technical sections which prove lemmas needed for the proof of the main results. Section 5 proves some important lemmas and closes with the proof of Theorem 1.3. Section 6 proves an extension of Theorem 1.3 to \mathbb{C} and \mathbb{H} . Section 7 proves a strong result, Theorem 7.3, for verifying whether a left module is real, which will be used for the Real Radical Algorithm. Section 8 is a technical section discussing left Gröbner bases. Section 9 presents the Real Radical Algorithm mentioned in Theorem 1.4 and proves its nice properties.

2. RIGHT CHIP SPACES AND FACTORIZATION OF MONOMIALS

We now introduce a natural class of monomials needed for the proofs, chip sets. Further, the Real Radical Algorithm described in Theorem 1.4 makes extensive use of chip sets, which makes said algorithm very efficient.

Given monomials $m_1, m_2 \in \mathcal{M}^{\nu \times \ell}$, we say that m_2 **right divides** m_1 , or that m_2 is a **right chip** of m_1 , if $m_1 = w m_2$ for some $w \in \langle x, x^* \rangle$.

If $w \neq 1$, we say the division is **proper** or that m_2 is a **proper right chip**.

Example 2.1. If

$$m_1 = e_2 \otimes x_1 x_2 x_3 \quad \text{and} \quad m_2 = e_2 \otimes x_2 x_3,$$

then $x_1 m_2 = m_1$, so m_2 is a proper right chip of m_1 .

A **right chip space** $\mathfrak{C} \subseteq \mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle$ is a space spanned by monomials m such that if $m \in \mathfrak{C}$, then so are all of its right chips. A right chip space is **finite** if it is finite dimensional.

The space of NC polynomials has a rigid structure which makes finding sums of squares representations easy. For example, Klep and Povh [18] showed that to verify that a NC polynomial p is a sum of squares, one needs only to use the right chips of the terms of p . In this section we prove some basic results about right chip spaces which will be useful in proving the main results of this article.

2.1. Constant Matrices in the Complement of a Full Right Chip Space. The element $1 \in \mathbb{R} \langle x, x^* \rangle$ right divides any monomial in $\mathbb{R}^{1 \times 1} \langle x, x^* \rangle = \mathbb{R} \langle x, x^* \rangle$, hence $1 \in \mathfrak{C}$ for any right chip space $\mathfrak{C} \subseteq \mathbb{R} \langle x, x^* \rangle$. For dimensions $\ell > 1$, however, not all right chip spaces contain all constants. Define $\Gamma(\mathfrak{C})$ to be

$$\Gamma(\mathfrak{C}) := \{j \mid e_j \otimes 1 \in \mathfrak{C}\} \subseteq \{1, \dots, \ell\}.$$

Lemma 2.2. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space. Then $\mathbb{R} \langle x, x^* \rangle \mathfrak{C}$ is equal to*

$$\mathbb{R} \langle x, x^* \rangle \mathfrak{C} = \bigoplus_{j \in \Gamma(\mathfrak{C})} e_j \otimes \mathbb{R} \langle x, x^* \rangle.$$

Proof. If $e_j \otimes w \in \mathfrak{C}$ for some $w \in \langle x, x^* \rangle$, then since \mathfrak{C} is a full right chip space, $e_j \otimes 1 \in \mathfrak{C}$. The result is clear from here. \square

Of interest as well are spaces of the form $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \subseteq \mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$.

Lemma 2.3. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space. Then $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$ is equal to*

$$\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C} = \bigoplus_{i,j \in \Gamma(\mathfrak{C})} E_{ij} \otimes \mathbb{R} \langle x, x^* \rangle.$$

Proof. This is clear from Lemma 2.2. \square

Lemma 2.4. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space, and let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a left module generated by polynomials in $\mathbb{R} \langle x, x^* \rangle \mathfrak{C}$. Then*

$$(\mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}) \cap \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C} = \mathfrak{C}^* I + I^* \mathfrak{C}.$$

Proof. Let Θ be the space defined by

$$\Theta = \bigoplus_{j \notin \Gamma(\mathfrak{C})} e_j \otimes \mathbb{R}\langle x, x^* \rangle.$$

By Lemma 2.2, $\mathbb{R}^{1 \times \ell}\langle x, x^* \rangle = \mathbb{R}\langle x, x^* \rangle \mathfrak{C} \oplus \Theta$, and

$$\begin{aligned} \mathfrak{C}^* \mathbb{R}\langle x, x^* \rangle \mathfrak{C} &= \bigoplus_{i,j \in \Gamma(\mathfrak{C})} E_{ij} \otimes \mathbb{R}\langle x, x^* \rangle, & \Theta^* \mathfrak{C} &= \bigoplus_{\substack{i \notin \Gamma(\mathfrak{C}) \\ j \in \Gamma(\mathfrak{C})}} E_{ij} \otimes \mathbb{R}\langle x, x^* \rangle \\ \mathfrak{C}^* \Theta &= \bigoplus_{\substack{i \in \Gamma(\mathfrak{C}) \\ j \notin \Gamma(\mathfrak{C})}} E_{ij} \otimes \mathbb{R}\langle x, x^* \rangle, & \Theta^* \Theta &= \bigoplus_{i,j \notin \Gamma(\mathfrak{C})} E_{ij} \otimes \mathbb{R}\langle x, x^* \rangle. \end{aligned}$$

Therefore,

$$(2.1) \quad \mathbb{R}^{\ell \times \ell}\langle x, x^* \rangle = \mathfrak{C}^* \mathbb{R}\langle x, x^* \rangle \mathfrak{C} \oplus \Theta^* \mathfrak{C} \oplus \mathfrak{C}^* \Theta \oplus \Theta^* \Theta.$$

Let $\iota_1, \dots, \iota_i, \dots \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C}$ generate I . Each $\iota \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}$ is of the form

$$\iota = \sum_i^{\text{finite}} (p_i^* \iota_i + \iota_i^* q_i),$$

for some $p_i, q_i \in \mathbb{R}^{1 \times \ell}\langle x, x^* \rangle$. Decompose each p_i as $\phi_{p_i} + \theta_{p_i}$ and each q_i as $\phi_{q_i} + \theta_{q_i}$ so that $\phi_{p_i}, \phi_{q_i} \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C}$ and $\theta_{p_i}, \theta_{q_i} \in \Theta$. Then

$$(2.2) \quad \iota = \sum_i^{\text{finite}} (\phi_{p_i}^* \iota_i + \iota_i^* \phi_{q_i}) + \sum_i^{\text{finite}} (\theta_{p_i}^* \iota_i) + \sum_i^{\text{finite}} (\iota_i^* \theta_{q_i}),$$

so that the first sum of (2.2) is in $\mathfrak{C}^* \mathbb{R}\langle x, x^* \rangle \mathfrak{C}$, the second in $\Theta^* \mathfrak{C}$, and the third in $\mathfrak{C}^* \Theta$. If $\iota \in \mathfrak{C}^* \mathbb{R}\langle x, x^* \rangle \mathfrak{C}$, by (2.1), ι is equal to the first sum in (2.2), which is an element of $\mathfrak{C}^* I + I^* \mathfrak{C}$. \square

2.2. Unique Factorization of Monomials. If $w \in \langle x, x^* \rangle$ and $0 \leq d \leq |w|$, one can factor w uniquely as $w = w_1 w_2$, where $w_1, w_2 \in \langle x, x^* \rangle$ with $|w_1| = d$ and $|w_2| = |w| - d$. The following lemma generalizes this fact to $\mathbb{R}^{\nu \times \ell}\langle x, x^* \rangle$.

Lemma 2.5. *Let $m = E_{ij} \otimes w \in \mathcal{M}^{\nu \times \ell}\langle x, x^* \rangle$ and $w \in \langle x, x^* \rangle$. For each $0 \leq d \leq |m|$, there exists a factorization of m as $m = m_1^* m_2$, where $m_1 \in \mathcal{M}^{1 \times \nu}$, $m_2 \in \mathcal{M}^{1 \times \ell}$, $\deg(m_1) = d$, and $\deg(m_2) = |m| - d$. Further, this factorization is uniquely determined, up to scalar multiplication, by $m_1 = e_i \otimes w_1^*$, $m_2 = e_j \otimes w_2$, where $w = w_1 w_2$, $w_1, w_2 \in \langle x, x^* \rangle$, with $|w_1| = d$ and $|w_2| = |m| - d$.*

Proof. It is clear that m can be factored as $m = (e_i \otimes w_1^*)^*(e_j \otimes w_2) = E_{ij} \otimes w$, where $w_1, w_2 \in \langle x, x^* \rangle$ with $|w_1| = d$ and $|w_2| = |m| - d$. Conversely, suppose $m = m_1^* m_2$, where

$$m_1 = \sum_{\rho=1}^{\nu} \sum_{u \in \langle x, x^* \rangle} A_{\rho,u} e_{\rho} \otimes u \quad \text{and} \quad m_2 = \sum_{\sigma=1}^{\ell} \sum_{v \in \langle x, x^* \rangle} B_{\sigma,v} e_{\sigma} \otimes v,$$

for some $A_{\rho,u}, B_{\sigma,v} \in \mathbb{R}$. Then,

$$\begin{aligned} m_1^* m_2 &= \sum_{\rho=1}^{\nu} \sum_{\sigma=1}^{\ell} \sum_{u \in \langle x, x^* \rangle} \sum_{v \in \langle x, x^* \rangle} A_{\rho,u} B_{\sigma,v} E_{\rho\sigma} \otimes u^* v \\ (2.3) \quad &= \sum_{\rho=1}^{\nu} \sum_{\sigma=1}^{\ell} E_{\rho\sigma} \otimes \left(\sum_{u \in \langle x, x^* \rangle} A_{\rho,u} u \right)^* \left(\sum_{v \in \langle x, x^* \rangle} B_{\sigma,v} v \right) \\ &= E_{ij} \otimes w. \end{aligned}$$

The terms of (2.3) with $\rho = i$ and $\sigma = j$ are equal to $E_{ij} \otimes w_1^* w_2$, which implies, by uniqueness of the factorization of w , that $A_{i,u} = B_{j,v} = 0$, for $u \neq w_1^*$ and $v \neq w_2$, and $A_{i,w_1^*} B_{j,w_2} = 1$. The terms of (2.3) with $\rho \neq i$ and $\sigma = j$ are equal to 0, which implies that each $A_{\rho,u} = 0$ for $\rho \neq i$. Similarly, each $B_{\sigma,v} = 0$ for $\sigma \neq j$. Therefore $m_1 = A_{i,w_1^*}(e_i \otimes w_1^*)$ and $m_2 = (1/A_{i,w_1^*})(e_j \otimes w_2)$. \square

Given a right chip space $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$, there are some special factorizations of monomials in $\mathcal{M}^{1 \times \ell}$ and $\mathcal{M}^{\ell \times \ell}$ which will be useful.

Lemma 2.6. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space. Each monomial $m \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$ has a unique word $w \in \langle x, x^* \rangle$ of minimum length and a unique right chip $\bar{m} \in \mathfrak{C}$ such that $m = w\bar{m}$.*

Proof. Each monomial in $\mathbb{R} \langle x, x^* \rangle \mathfrak{C}$ is of the form $w\bar{m}$, with $w \in \langle x, x^* \rangle$ and $\bar{m} \in \mathfrak{C}$. Uniqueness of the minimal $w \in \langle x, x^* \rangle$ follows from Lemma 2.5. \square

Lemma 2.7. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space. A monomial $m \in \mathcal{M}^{1 \times \ell}$ is in the set $\mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$ if and only if it can be expressed as $m = w\bar{m}$, where $\bar{m} \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ and $w \in \langle x, x^* \rangle$. Further, this representation is unique.*

Proof. Decompose $m \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$ as in Lemma 2.6 as $m = \hat{w}\hat{m}$, where $\hat{m} \in \mathfrak{C}$ and \hat{w} is as small as possible. We cannot have $\hat{w} = 1$ since $m \notin \mathfrak{C}$, so decompose \hat{w} as $\hat{w}_1 \hat{w}_2$, where $|\hat{w}_2| = 1$. Then $m = \hat{w}_1(\hat{w}_2 \hat{m})$, and by minimality of \hat{w} , $\bar{m} = \hat{w}_2 \hat{m} \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$.

Conversely, it is a contradiction to have $w\bar{m} \in \mathfrak{C}$ for some $w \in \langle x, x^* \rangle$ and $\bar{m} \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ since $\bar{m} \notin \mathfrak{C}$ would be a right chip of $w\bar{m} \in \mathfrak{C}$.

To show uniqueness, suppose $w_1\bar{m}_1 = w_2\bar{m}_2 \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$, where $w_1, w_2 \in \langle x, x^* \rangle$ and $\bar{m}_1, \bar{m}_2 \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$, and suppose $|w_1| \leq |w_2|$. If $|w_1| < |w_2|$, then decompose w_2 as $w_2 = w_1u$ for some $u \in \langle x, x^* \rangle$ with $|u| > 0$. Then $\bar{m}_1 = u\bar{m}_2$. Decompose \bar{m}_1 as $u_1u_2\bar{m}_2$, where $u = u_1u_2$, $u_1, u_2 \in \langle x, x^* \rangle$, and $|u_1| = 1$, so that $u_2\bar{m}_2 \in \mathfrak{C}$. Therefore $\bar{m}_2 \in \mathfrak{C}$, which is a contradiction. Therefore $|w_1| = |w_2|$, and by Lemma 2.5, $w_1 = w_2$ and $\bar{m}_1 = \bar{m}_2$. \square

Lemma 2.8. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space. A monomial $m \in \mathcal{M}^{\ell \times \ell}$ is in the space $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$ if and only if it can be expressed as $m = \bar{m}_1^* w \bar{m}_2$, where $\bar{m}_1, \bar{m}_2 \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ and $w \in \langle x, x^* \rangle$. Further, this representation is unique.*

Proof. First, $m \in \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$ if and only if it can be expressed as a^*bc , where $a, c \in \mathfrak{C}$ and $b \in \langle x, x^* \rangle$. Next, either $bc \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, in which case $a^*bc \in \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, or by Lemma 2.7, bc can be uniquely expressed as $bc = b_1(b_2c)$, where $b = b_1b_2$, $b_2c \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$, and $|b_1| > 0$. Next, either $b_1^*a \in \mathfrak{C}$, in which case $a^*bc \in \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, or by Lemma 2.7, b_1^*a can be uniquely expressed as $b_1^*(b_3^*a)$, where $b_1 = b_3b_4$ and $b_3^*a \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$. In the case that $a^*bc \in \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, we see that $a^*bc = (b_3^*a)^*b_4(b_2c)$, with $b_3^*a, b_2c \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ and $b_4 \in \langle x, x^* \rangle$.

Next, suppose $\bar{m}_1^* w \bar{m}_2 = t^*uv$, where $\bar{m}_1, \bar{m}_2 \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$, $t, v \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, and $w, u \in \langle x, x^* \rangle$. If $|t| > |\bar{m}_1|$, then Lemma 2.5 implies that \bar{m}_1 right divides t properly, which implies by Lemma 2.5 that $t \notin \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, which is a contradiction. Therefore, $|t| \leq |\bar{m}_1|$, and similarly, $|v| \leq |\bar{m}_2|$. If $|t| < |\bar{m}_1|$, then by Lemma 2.5, t properly divides \bar{m}_1 on the right, so Lemma 2.7 implies that $t \in \mathfrak{C}$. Similarly, if $|v| < |\bar{m}_2|$, then $v \in \mathfrak{C}$. In the case that $t, v \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$, we see that $|t| = |\bar{m}_1|$ and $|v| = |\bar{m}_2|$, which implies, by Lemma 2.5, that $t = \bar{m}_1$ and $v = \bar{m}_2$, and further, $w = u$. This gives uniqueness. Also, notice that $\bar{m}_1^* w \bar{m}_2 \notin \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$ since if $t, v \in \mathfrak{C}$, then $|t| < |\bar{m}_1|$, $|v| < |\bar{m}_2|$, and so $|u| \geq 2$. \square

3. \mathfrak{C} -ORDERS AND \mathfrak{C} -BASES

Now we turn to orders on monomials. This is a subject familiar to those who work with Gröbner bases. However, it turns out that to take advantage of the structure of right chip spaces, we need to define an order different from the admissible orders used with Gröbner bases (see § 8 for more on left admissible orders.)

Given a total order \prec on $\mathcal{M}^{\nu \times \ell}$, we say that the **leading monomial** of a polynomial p , denoted $\text{lm}(p)$, is the highest monomial appearing in p according to \prec . We call a polynomial **monic** if its leading monomial

has coefficient 1. Given a set $I \subseteq \mathbb{R}^{1 \times \ell}$, let $\text{lm}(I)$ be the set of leading monomials of elements of I , and let $\text{Nlm}(I) := \mathcal{M}^{1 \times \ell} \setminus \text{lm}(I)$.

Lemma 3.1. *Let \prec be a total order on monomials in $\mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle$, and let $p_1, \dots, p_k \in \mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle \setminus \{0\}$. Suppose $\text{lm}(p_1) \prec \dots \prec \text{lm}(p_k)$. Then the leading monomial of $p_1 + \dots + p_k$ is $\text{lm}(p_k)$. In particular, $p_1 + \dots + p_k \neq 0$.*

Proof. Straightforward. \square

For right chip spaces \mathfrak{C} , we would like to find an order on $\mathcal{M}^{1 \times \ell}$ such $a \prec b$ whenever $a \in \mathfrak{C}$ and $b \notin \mathfrak{C}$. To do this, we introduce \mathfrak{C} -orders.

First, we say a total order \prec on $\langle x, x^* \rangle$ is a **degree order** if $a \prec b$ holds whenever $|a| < |b|$.

Next, let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space. Let \prec_0 be a degree order on $\langle x, x^* \rangle$. We say that $\prec_{\mathfrak{C}}$ is a **\mathfrak{C} -order (induced by \prec_0)** if $\prec_{\mathfrak{C}}$ is a total order on $\mathcal{M}^{1 \times \ell}$ such that if $a, b \in \mathcal{M}^{1 \times \ell}$, then $a \prec_{\mathfrak{C}} b$ if one of the following hold

- (1) $a \in \mathfrak{C}$ and $b \notin \mathfrak{C}$,
- (2) $a \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$ and $b \notin \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$,
- (3) $a = a_1 a_2, b = b_1 b_2$, where $a_2, b_2 \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$, $a_1, b_1 \in \langle x, x^* \rangle$, and $a_1 \prec_0 b_1$,
- (4) $a = w a_2, b = w b_2$, where $a_2, b_2 \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$, $w \in \langle x, x^* \rangle$, and $a_2 \prec_{\mathfrak{C}} b_2$.

The above conditions in and of themselves only define a partial order. By definition, a \mathfrak{C} order $\prec_{\mathfrak{C}}$ is defined in some way among the elements of \mathfrak{C} , $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$, and $\mathbb{R}^{1 \times \ell} \setminus \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$ respectively to make it a total order.

Lemma 3.2. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space and let $\prec_{\mathfrak{C}}$ be a \mathfrak{C} -order induced by a degree order \prec_0 . If $q \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ and $p \in \mathbb{R} \langle x, x^* \rangle \setminus \{0\}$, then the leading monomial of pq is $\text{lm}(p) \text{lm}(q)$, where $\text{lm}(p)$ is the leading monomial of p according to \prec_0 and $\text{lm}(q) \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ is the leading monomial of q according to $\prec_{\mathfrak{C}}$.*

Proof. First, $\text{lm}(q) \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ since $q \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ and the elements of \mathfrak{C} are less than the elements of $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ under $\prec_{\mathfrak{C}}$. Consider the case where p is a monomial. Let $\phi \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$ be a monomial appearing in q . If $\phi \in \mathfrak{C}$, then either $p\phi \in \mathfrak{C}$, or by Lemma 2.7, $p\phi = p_1 p_2 \phi$, where $p_1, p_2 \in \langle x, x^* \rangle$ are such that $p = p_1 p_2$, and $p_2 \phi \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$. In this case, $|p_1| < |p|$. In either case where $\phi \in \mathfrak{C}$, we see that $p\phi \prec_{\mathfrak{C}} p \text{lm}(q)$. If, $\phi \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$, but $\phi \neq \text{lm}(q)$, then since $\text{lm}(q)$ is the leading monomial, $\phi \prec_{\mathfrak{C}} \text{lm}(q)$.

Therefore $p\phi \prec_{\mathfrak{C}} p\text{lm}(q)$. Therefore the leading monomial of pq is $p\text{lm}(q)$.

The general case follows from Lemma 3.1. \square

3.1. \mathfrak{C} -Bases. Given a \mathfrak{C} -order and a left module I generated by elements of $\mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, we can construct what we call a \mathfrak{C} -basis.

Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space and let $\prec_{\mathfrak{C}}$ be a \mathfrak{C} -order. Let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a left module generated by polynomials in $\mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$. We say that a pair of sets $(\{\iota_i\}_{i \in A}, \{\vartheta_j\}_{j \in B})$ is a \mathfrak{C} -basis for I if $\{\iota_i\}_{i \in A}$ is a maximal set of monic polynomials in $I \cap (\mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C})$ with distinct leading monomials and if $\{\vartheta_j\}_{j \in B}$ is a maximal (possibly empty) set of monic polynomials in $I \cap \mathfrak{C}$ with distinct leading monomials.

Lemma 3.3. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space. Let $\{\iota_i\}_{i \in A} \subseteq \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ be a set of polynomials with distinct leading monomials, and let $\{\vartheta_j\}_{j \in B} \subseteq \mathfrak{C}$ be a set of polynomials with distinct leading monomials. The following are true of the polynomial q defined by*

$$q = \sum_i^{\text{finite}} p_i \iota_i + \sum_j^{\text{finite}} \alpha_j \vartheta_j,$$

where each $p_i \in \mathbb{R}\langle x, x^* \rangle$ and $\alpha_j \in \mathbb{R}$.

- (1) If $q \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$, then $\text{lm}(q) = \text{lm}(p_i) \text{lm}(\iota_i)$ for some i .
- (2) If $q \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, then each p_i is constant.
- (3) If $q \in \mathfrak{C}$, then each $p_i = 0$.
- (4) If $q = 0$, then each $p_i = 0$ and each $\alpha_j = 0$.

Proof. Fix a \mathfrak{C} -order. If any of the p_i are nonzero, by Lemmas 3.1 and 3.2, since all of the $\text{lm}(q_i)$ are distinct, the leading monomial of q is the maximal $\text{lm}(p_i) \text{lm}(q_i)$. The maximal $\text{lm}(p_i)$ has maximal length by definition of a \mathfrak{C} -order. If $q \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, then so is its leading monomial, in which case any nonzero $\text{lm}(p_i)$ must be equal to 1 by Lemma 2.7. Therefore, if $q \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, then each p_i is either 0 or is a nonzero constant. Further, if $q \in \mathfrak{C}$, then its leading monomial cannot be in $\mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$. In this case, all of the $p_i = 0$. Finally, if $q = 0$, then each of the $p_i = 0$ and further, by Lemma 3.1, the α_j must all be 0 as well. \square

Note that Lemma 3.3 (4) implies that the union of the two sets of a \mathfrak{C} -basis is a linearly independent set.

Lemma 3.4. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a finite right chip space and let $\prec_{\mathfrak{C}}$ be a \mathfrak{C} -order induced by some degree order. Let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a left*

module generated by polynomials in $\mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$ and let $(\{\iota_i\}_{i=1}^\mu, \{\vartheta_j\}_{j=1}^\sigma)$ be a \mathfrak{C} -basis for I . Each element of I can be represented uniquely as

$$(3.1) \quad \sum_{i=1}^{\mu} p_i \iota_i + \sum_{j=1}^{\sigma} \alpha_j \vartheta_j,$$

where each $p_i \in \mathbb{R}\langle x, x^* \rangle$ and $\alpha_j \in \mathbb{R}$.

Conversely, any pair of sets of monic polynomials $(\{\iota_i\}_{i=1}^\mu, \{\vartheta_j\}_{j=1}^\sigma)$ with distinct leading monomials such that any element of I can be expressed in the form (3.1) is a \mathfrak{C} -basis for I .

Proof. Every element of $I \cap \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$ has leading monomial equal to the leading monomial of an element of the \mathfrak{C} -basis, hence it follows that the \mathfrak{C} -basis spans $I \cap \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$. Further, if $\vartheta_j \in I \cap \mathfrak{C}$, then for each $w \in \langle x, x^* \rangle$ of length 1 we have $w\vartheta_j \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, which is the span of the \mathfrak{C} basis. Since the \mathfrak{C} -basis generates I , this implies that every element of I can be expressed in the form (3.1). Further, uniqueness follows from Lemma 3.3.

Conversely, suppose $(\{\iota_i\}_{i=1}^\mu, \{\vartheta_j\}_{j=1}^\sigma)$ is a pair of sets of monic polynomials with distinct leading monomials such that any element of I can be expressed in the form (3.1). Let $\theta \in I \cap \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$ be equal to

$$\theta = \sum_{i=1}^{\mu} p_i \iota_i + \sum_{j=1}^{\sigma} \alpha_j \vartheta_j.$$

Lemma 3.3 implies that if $\theta \neq 0$ then it cannot have a distinct leading monomial from the ι_i and ϑ_j . Therefore the pair $(\{\iota_i\}_{i=1}^\mu, \{\vartheta_j\}_{j=1}^\sigma)$ is a \mathfrak{C} -basis. \square

4. DOUBLE \mathfrak{C} -ORDERS

In addition to ordering elements of $\mathcal{M}^{1 \times \ell}$, we also want to order elements of $\mathcal{M}^{\ell \times \ell}$.

Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space. Let $\prec_{\mathfrak{C}}$ be a \mathfrak{C} -order. We say that $\prec_{\mathfrak{C} \times \mathfrak{C}}$ is a **double \mathfrak{C} -order (induced by $\prec_{\mathfrak{C}}$)** if $\prec_{\mathfrak{C} \times \mathfrak{C}}$ is a total order on $\mathcal{M}^{\ell \times \ell}$ such that given $a, b \in \mathcal{M}^{\ell \times \ell}$ we have $a \prec_{\mathfrak{C} \times \mathfrak{C}} b$ if one of the following hold

- (1) $a \in (\mathbb{R}^{1 \times \ell} \cap \mathfrak{C})^* \mathfrak{C}$ and $b \notin (\mathbb{R}^{1 \times \ell} \cap \mathfrak{C})^* \mathfrak{C}$,
- (2) $a \in \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$ and $b \notin \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$,
- (3) $a = a_1^* a_2$, $b = b_1^* b_2$, where $a_2, b_2 \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$, $a_1, b_1 \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$, and either
 - (a) $a_1 \prec_{\mathfrak{C}} b_1$, or
 - (b) $a_1 = b_1$ and $a_2 \prec_{\mathfrak{C}} b_2$.

The above conditions in and of themselves only define a partial order. By definition, $\prec_{\mathfrak{C} \times \mathfrak{C}}$ is a total order, so it is defined in some way beyond what has been stated to produce a total order.

Lemma 4.1. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space, let $\prec_{\mathfrak{C}}$ be a \mathfrak{C} -order, and let $\prec_{\mathfrak{C} \times \mathfrak{C}}$ be a double \mathfrak{C} -order induced by $\prec_{\mathfrak{C}}$. If $q \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ and $p \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$, then the leading monomial of p^*q is $\text{lm}(p)^* \text{lm}(q)$, where $\text{lm}(p)$ is the leading monomial of p according to $\prec_{\mathfrak{C}}$ and $\text{lm}(q) \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ is the leading monomial of q according to $\prec_{\mathfrak{C}}$.*

Proof. First note that $\text{lm}(q) \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ and $\text{lm}(p) \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$ by definition of \mathfrak{C} . By Lemma 2.8, $\text{lm}(p)^* \text{lm}(q)$ is in $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$. Let ϕ be a term of p and let ψ be a term of q . Consider two cases.

If $\psi \in \mathfrak{C}$, let $\phi = e_i \otimes w$. Then either $w\psi \in \mathfrak{C}$, in which case $\phi^*\psi \in (\mathbb{R}^{1 \times \ell} \cap \mathfrak{C})^* \mathfrak{C}$, or by Lemma 2.7, $w^*\psi = w_2^* w_1^* \psi$, where $w_1^* \psi \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$. In the first case, by definition $\phi^*\psi \prec_{\mathfrak{C} \times \mathfrak{C}} \text{lm}(p)^* \text{lm}(q)$. In the second case, either $e_i \otimes w_2 \in \mathfrak{C}$ so that $e_i \otimes w_2 \prec_{\mathfrak{C}} \text{lm}(p)$ or $e_i \otimes w_2 \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$, implying that $e_i \otimes w_2 \prec_{\mathfrak{C}} e_i \otimes_{\mathfrak{C}} w_1 w_2 \preceq_{\mathfrak{C}} \text{lm}(p)$. Either way, $\phi^*\psi = (e_i \otimes w_2)^* (w_1^* \psi) \prec_{\mathfrak{C} \times \mathfrak{C}} \text{lm}(p)^* \text{lm}(q)$.

The second case is that $\psi \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$. In this case, it must be that $\psi \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ since $q \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$. It follows easily that $\phi^*\psi \preceq_{\mathfrak{C} \times \mathfrak{C}} \text{lm}(p)^* \text{lm}(q)$ and is only equal if $\phi = \text{lm}(p)$ and $\psi = \text{lm}(q)$. \square

Lemma 4.2. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a finite right chip space, let $\prec_{\mathfrak{C}}$ be a \mathfrak{C} -order, and let $\prec_{\mathfrak{C} \times \mathfrak{C}}$ be a double \mathfrak{C} -order induced by $\prec_{\mathfrak{C}}$. Let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a left module generated by polynomials in $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$. Let $(\{\iota_i\}_{i=1}^{\mu}, \{\vartheta_j\}_{j=1}^{\sigma})$ be a \mathfrak{C} -basis for $I \cap \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$. Let $\{\tau_1, \dots, \tau_{\omega}\} = \text{Nlm}(I) \cap \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$.*

- (1) *Every element of $(\mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}) \cap \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$ can be represented as*

$$(4.1) \quad \sum_{i=1}^{\mu} \sum_{j=1}^{\mu} \iota_i^* p_{ij}^* \iota_j + \sum_{i=1}^{\omega} \sum_{j=1}^{\mu} \tau_i^* q_{ij}^* \iota_j + \sum_{i=1}^{\mu} \sum_{j=1}^{\omega} \iota_i^* r_{ij}^* \tau_j \\ + \sum_{i=1}^{\mu} (s_i^* \iota_i + \iota_i^* t_i) + \sum_{i=1}^{\sigma} (\alpha_i^* \vartheta_i + \vartheta_i^* \beta_i),$$

where $p_{ij}, q_{ij}, r_{ij} \in \mathbb{R} \langle x, x^* \rangle$, $s_i, t_i \in \mathfrak{C}$, and $\alpha_j, \beta_j \in \mathbb{R}^{1 \times \ell} \cap \mathfrak{C}$. Further, the p_{ij}, q_{ij} and r_{ij} are unique.

- (2) If (4.1) is in $\mathfrak{C}^*\mathbb{R}\langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}^*\mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, then its the leading polynomial is of the form $m^* \text{lm}(\iota_i)$ or $\text{lm}(\iota_i)^* m$ for some ι_i and some monomial $m \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$.
- (3) If (4.1) is in $\mathfrak{C}^*\mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, then $p_{ab} = q_{cd} = r_{ef} = 0$ for each $1 \leq a, b, d, e \leq \mu$ and $1 \leq c, f \leq \sigma$.

Proof. By Lemma 2.4, $(\mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}) \cap \mathfrak{C}^*\mathbb{R}\langle x, x^* \rangle \mathfrak{C} = \mathfrak{C}^* I + I^* \mathfrak{C}$, and consists of all polynomials of the form

$$(4.2) \quad \sum_{i=1}^{\mu} (a_i^* \iota_i + \iota_i^* b_i) + \sum_{j=1}^{\sigma} (\alpha_j^* \vartheta_j + \vartheta_j^* \beta_j),$$

where $a_i, b_i, \alpha_j, \beta_j \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C}$. If $i \in \Gamma(\mathfrak{C})$ and $w \in \langle x, x^* \rangle$, either $|w| = 0$ or $w = w_1 w_2$, where $w_1, w_2 \in \langle x, x^* \rangle$ with $|w_1| = 1$. In the second case, for each ϑ_j , we see that $(e_i \otimes w_1 w_2)^* \vartheta_j = (e_i \otimes w_2)^* (w_1^* \vartheta_j)$. Since $w_1^* \vartheta_j \in I \cap \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, then $w_1^* \vartheta_j$ is in the span of the \mathfrak{C} -basis. Reducing in this way, we can take the α_i and β_i in (4.1) to be elements of $(\mathbb{R}^{1 \times \ell} \otimes 1) \cap \mathfrak{C}$.

Next, consider

$$\sum_{i=1}^{\mu} (a_i^* \iota_i + \iota_i^* b_i).$$

If $\text{lm}(a_i) \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$, then by Lemma 2.7, it can be decomposed as $\text{lm}(a_i) = w m$, where $w \in \langle x, x^* \rangle$ and $m \in \mathbb{R}\langle x, x^* \rangle_1 \setminus \mathfrak{C}$. Let $A \in \mathbb{R}$ be the coefficient of $\text{lm}(a_i)$ in a . By construction, m is either equal to some $\text{lm}(\iota_j)$ or some τ_j . In the first case, we see that $a_i = (a_i - A w \iota_j) + w \iota_j$, so that $a_i - A w \iota_j$ has a smaller leading monomial than a_i . In the latter case, $a_i = (a_i - w \tau_j) + w \tau_j$, so that $a_i - w \tau_j$ has a smaller leading monomial than a_i . Since \mathfrak{C} is finite dimensional, we can continue this until we decompose each a_i , and likewise each b_i , as

$$a_i = \sum_{j=1}^{\mu} \tilde{a}_{ij} \iota_j + \sum_{j=1}^{\sigma} q_{ij} \tau_j + s_i \quad \text{and} \quad b_i = \sum_{j=1}^{\mu} \tilde{b}_{ij} \iota_j + \sum_{j=1}^{\sigma} r_{ij}^* \tau_j + t_i,$$

where $\tilde{a}_{ij}, q_{ij}, \tilde{b}_{ij}, r_{ij} \in \mathbb{R}\langle x, x^* \rangle$ and $s_i, t_i \in \mathfrak{C}$. Therefore

$$\begin{aligned} \sum_{i=1}^{\mu} (a_i^* \iota_i + \iota_i^* b_i) &= \sum_{i=1}^{\mu} \sum_{j=1}^{\mu} \iota_i^* (\tilde{a}_{ij}^* + \tilde{b}_{ij}) \iota_j + \sum_{i=1}^{\omega} \sum_{j=1}^{\mu} \tau_i^* q_{ij}^* \iota_j \\ &\quad + \sum_{i=1}^{\mu} \sum_{j=1}^{\omega} \iota_i^* r_{ij}^* \tau_j + \sum_{i=1}^{\mu} (s_i^* \iota_i + \iota_i^* t_i). \end{aligned}$$

Setting $p_{ij} = \tilde{a}_{ij} + \tilde{b}_{ij}^*$ gives (4.1).

Next, consider the leading monomial of (4.1). If $p_{ij} \neq 0$ for some ij , then by Lemmas 3.2 and 4.1, the leading monomial of $\iota_i^* p_{ij}^* \iota_j$ is

$$\text{lm}(\iota_i^* p_{ij}^* \iota_j) = \text{lm}(p_{ij} \iota_i)^* \text{lm}(\iota_j) = \text{lm}(\iota_i)^* \text{lm}(p_{ij})^* \text{lm}(\iota_j).$$

Similarly, the leading monomials of each nonzero $\tau_i^* q_{ij}^* \iota_j$ and $\iota_i^* r_{ij}^* \tau_j$ are

$$\text{lm}(\tau_i^* q_{ij}^* \iota_j) = \tau_i^* \text{lm}(q_{ij})^* \text{lm}(\iota_j)$$

and

$$\text{lm}(\iota_i^* r_{ij}^* \tau_j) = \text{lm}(\iota_i)^* \text{lm}(r_{ij})^* \tau_j.$$

All of these possible leading monomials are distinct by Lemma 2.8. The last line in (4.1) is in $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, so if (4.1) is not in $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, then its leading monomial must be of the form $m^* \text{lm}(\iota_i)$ or $\text{lm}(\iota_i)^* m$ for some ι_i . On the other hand, if the last line in (4.1) is in $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, then we see that each $p_{ab} = q_{cd} = r_{ef} = 0$ since otherwise its leading monomial would lie outside of $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$. By linearity, this implies that the representation in (4.1) must be unique. \square

5. POSITIVE LINEAR FUNCTIONALS ON $\mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$

The main theorem of this paper, Theorem 5.10, will be proved at the end of this section. We now discuss linear functionals and prove some important lemmas which will be used in the proof of the main result.

A (\mathbb{R}) -linear functional L on $W \subseteq \mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$ is **symmetric** if $L(\omega^*) = L(\omega)$ for each pair $\omega, \omega^* \in W$. A linear functional L on a subspace $W \subseteq \mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$ is **positive** if it is symmetric and if $L(w^* w) \geq 0$ for each $w^* w \in W$.

Lemma 5.1. *If L is a positive linear functional on $\mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$, then $I := \{\vartheta \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle \mid L(\vartheta^* \vartheta) = 0\}$ is a real left module and $L(\mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}) = \{0\}$.*

Proof. The space $\mathbb{R}^{\ell \times 1} I$ is spanned by polynomials of the form $b^* a$, where $a \in I$ and $b \in \mathbb{R}^{1 \times \ell}$. For each $\xi \in \mathbb{R}$, by positivity of L ,

$$L([a + \xi b]^* [a + \xi b]) = 2\xi L(b^* a) + \xi^2 L(b^* b) \geq 0,$$

which implies that $L(b^* a) = 0$. Therefore, $L(\mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}) = \{0\}$. Next, if $q \in \mathbb{R} \langle x, x^* \rangle$, then for each $\xi \in \mathbb{R}$,

$$L([a + \xi q^* q a]^* [a + \xi q^* q a]) = 2\xi L(a^* q^* q a) + \xi^2 L(a^* q^* q q^* q a) \geq 0,$$

which implies that $L(a^* q^* q a) = 0$. Therefore $q a \in I$. Further, if $c \in I$, then for each $\xi \in \mathbb{R}$,

$$L([a + \xi c]^* [a + \xi c]) = 2\xi L(a^* c) \geq 0,$$

which implies that $L(a^*c) = 0$. Therefore, $a + c \in I$, which implies that I is a left module. Finally suppose $\sum_i^{\text{finite}} p_i^* p_i \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}$. Then

$$L\left(\sum_i^{\text{finite}} p_i^* p_i\right) = \sum_i^{\text{finite}} L(p_i^* p_i) = 0,$$

which implies that each $L(p_i^* p_i) = 0$. Therefore each $p_i \in I$, which implies that I is real. \square

Let $W \subseteq \mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$ be a vector subspace and let L be a positive linear functional on W . Suppose

$$\{\omega \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle \mid \omega^* \omega \in W\} = J \oplus T$$

where $J, T \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ are vector subspaces with

$$J := \{\vartheta \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle \mid \vartheta^* \vartheta \in W \text{ and } L(\vartheta^* \vartheta) = 0\}.$$

An extension \bar{L} of L to a space $U \supseteq W$ is a **flat extension** if \bar{L} is positive and if

$$\{u \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle \mid u^* u \in U\} = I \oplus T$$

where

$$I = \{\iota \in \mathbb{R}^{1 \times \ell} \mid \iota^* \iota \in U \text{ and } \bar{L}(\iota^* \iota) = 0\}.$$

Proposition 5.2. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a finite right chip space. Let L be a positive linear functional on $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$.*

- (1) *There exists a positive extension of L to the space $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_2 \mathfrak{C}$ if and only if whenever $\vartheta \in \mathfrak{C}$ satisfies $L(\vartheta^* \vartheta) = 0$, then $L(b^* c \vartheta) = 0$ for each polynomial $b \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$ and each $c \in \mathbb{R} \langle x, x^* \rangle$ such that $c \vartheta \in \mathfrak{C}$.*
- (2) *If there exists a positive extension of L to the space $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_2 \mathfrak{C}$, then there exists a unique flat extension \bar{L} of L to $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$. In this case, the space*

$$\{\theta \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \mid \bar{L}(\theta^* \theta) = 0\}$$

is generated as a left module by the set

$$(5.1) \quad \{\iota \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \mid L(b^* \iota) = 0 \text{ for every } b \in \mathfrak{C}\}.$$

- (3) *Given the existence of a flat extension \bar{L} to $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$, there exists a flat extension of \bar{L} to all of $\mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$.*

Proof. First, suppose there exists a positive extension \tilde{L} of L to the space $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_2 \mathfrak{C}$. Let $\vartheta \in \mathfrak{C}$ satisfy $L(\vartheta^* \vartheta) = 0$. If $\tilde{c} \vartheta \in \mathfrak{C}$, with

$\tilde{c} = \mathbb{R}\langle x, x^* \rangle_1$ then $\tilde{c}^* \tilde{c} \vartheta \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$. For each $\xi \in \mathbb{R}$, since \tilde{L} is positive,

$$\tilde{L}([\vartheta + \xi \tilde{c}^* \tilde{c} \vartheta]^* [\vartheta + \xi \tilde{c}^* \tilde{c} \vartheta]) = 2\xi L(\vartheta^* \tilde{c}^* \tilde{c} \vartheta) + \xi^2 \tilde{L}(\vartheta^* \tilde{c}^* \tilde{c} \tilde{c}^* \tilde{c} \vartheta) \geq 0,$$

which implies that $L([\tilde{c} \vartheta]^* [\tilde{c} \vartheta]) = 0$. We can then extend this to show that if $c \vartheta \in \mathfrak{C}$ for any $c \in \mathbb{R}\langle x, x^* \rangle$ then $L([c \vartheta]^* [c \vartheta]) = 0$. Further, if $b \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, then for each $\xi \in \mathbb{R}$, since \tilde{L} is positive,

$$\tilde{L}([c \vartheta + \xi b]^* [c \vartheta + \xi b]) = 2\xi L(b^* c \vartheta) + \xi^2 \tilde{L}(b^* b) \geq 0,$$

which implies that $L(b^* c \vartheta) = 0$.

Conversely, let \mathfrak{C} be decomposed as $J \oplus T$, where

$$J = \{\vartheta \in \mathfrak{C} \mid L(\vartheta^* \vartheta) = 0\},$$

and $T \subseteq \mathfrak{C}$ is some complementary subspace, and suppose $L(b^* c \vartheta) = 0$ for each $\vartheta \in J$, each $b \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, and each $c \in \mathbb{R}\langle x, x^* \rangle$ such that $c \vartheta \in \mathfrak{C}$.

Define an inner product on T by $\langle a, b \rangle = L(b^* a)$. This inner product is well defined since L is symmetric and is positive on squares of T . Let τ_1, \dots, τ_μ be an orthonormal basis for T according to this inner product. If $m \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ is a monomial, then consider the polynomial p_m defined by

$$(5.2) \quad p_m := m - \sum_{j=1}^{\mu} L(\tau_j^* m) \tau_j.$$

If $b \in \mathfrak{C}$, then $b = \vartheta + \sum_{k=1}^{\mu} \beta_k \tau_k$ for some $\vartheta \in J$ and $\beta_k \in \mathbb{R}$. We see that

$$L(b^* p_m) = L(\vartheta^* p_m) + \sum_{k=1}^{\mu} \beta_k L(\tau_k^* p_m) - \sum_{j=1}^{\mu} \sum_{k=1}^{\mu} \beta_k L(\tau_j^* m) L(\tau_k^* \tau_j) = 0.$$

Therefore p_m is in the set (5.1). Also note that a flat extension \bar{L} of L must satisfy $\bar{L}(p_m^* p_m) = 0$ since the equation

$$\bar{L} \left(\left[p_m + \sum_{j=1}^{\mu} \gamma_j \tau_j \right]^* \left[p_m + \sum_{j=1}^{\mu} \gamma_j \tau_j \right] \right) = \sum_{j=1}^{\mu} \gamma_j^2 L(\tau_j^* \tau_j) + \bar{L}(p_m^* p_m) = 0$$

has only one solution in γ and $\bar{L}(p_m^* p_m) = 0$: each $\gamma_i = 0$ and $\bar{L}(p_m^* p_m) = 0$.

Next, consider $w\psi \in \mathbb{R}\langle x, x^* \rangle_d \mathfrak{C}$, where $w = w_1 w_2$, with $|w_2| = 1$, and $\psi \in \mathfrak{C}$. We see that either $w_2 \psi \in \mathfrak{C}$, or $w_2 \psi \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$. In either case, $w_2 \psi = \iota + \zeta$, where $\iota \in \text{Span}(\{p_m \mid m \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}\})$ and $\zeta \in \mathfrak{C}$. Therefore

$$w\psi = w_1 \iota + w_1 \zeta,$$

so that $w_1\iota \in \mathbb{R}\langle x, x^* \rangle (\text{Span}[\{p_m\}])$ and $w_1\zeta \in \mathbb{R}\langle x, x^* \rangle_{d-1}\mathfrak{C}$. By induction, this implies that each element of $\mathbb{R}\langle x, x^* \rangle \mathfrak{C}$ is in $\mathbb{R}\langle x, x^* \rangle (\text{Span}[\{p_m\}]) + \mathfrak{C}$. Lemma 3.3 further implies that

$$\mathbb{R}\langle x, x^* \rangle \mathfrak{C} = \mathbb{R}\langle x, x^* \rangle (\text{Span}[\{p_m\}]) \oplus \mathfrak{C}.$$

Let I be the left module generated by $(\mathbb{R}\langle x, x^* \rangle \text{Span}[\{p_m\}]) \oplus J$. Let ι be in the set (5.1). Since $\iota \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$ we can decompose it as

$$\iota = \sum_{m \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}} \alpha_m p_m + \vartheta,$$

where each $\alpha_m \in \mathbb{R}$ and $\vartheta \in \mathfrak{C}$. We see that $L(\vartheta^* \vartheta) = L(\vartheta^* \iota) = 0$, which implies that $\vartheta \in J$. Therefore, $\iota \in I$, which implies that I contains the set (5.1).

Conversely, let $\vartheta \in J$. By assumption ϑ is in the set (5.1). Further, if $c \in \langle x, x^* \rangle$ has length 1, then $c\vartheta \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$. By assumption, we must have $c\vartheta$ in (5.1). Therefore the generators of I are in (5.1), which implies that I is the left module generated by (5.1). Further, since $c\vartheta$ is in the set (5.1), $c\vartheta$ must be in the span of the p_m and J . Therefore

$$I = \mathbb{R}\langle x, x^* \rangle \text{Span}(\{p_m\}) \oplus J \quad \text{and} \quad \mathbb{R}\langle x, x^* \rangle \mathfrak{C} = I \oplus T.$$

Define an inner product linearly on $\mathbb{R}\langle x, x^* \rangle \mathfrak{C}/I$ to be

$$\langle [\tau_i], [\tau_j] \rangle := \langle \tau_i, \tau_j \rangle = L(\tau_i^* \tau_j),$$

where τ_1, \dots, τ_μ are the orthonormal basis elements of T previously defined. Since $I \cap T = \{0\}$, this inner product is well defined.

Let \bar{L} be a linear functional on $\mathfrak{C}^* \mathbb{R}\langle x, x^* \rangle \mathfrak{C}$ defined by

$$\bar{L}(b^* a) := \langle [a], [b] \rangle.$$

Clearly \bar{L} is positive and symmetric. Further, given an element $b^* p a \in \mathfrak{C}^* \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$, with $a, b \in \mathfrak{C}$ and $p \in \mathbb{R}\langle x, x^* \rangle_1$, decompose pa as $pa = \iota_a + \tau_a$ and b as $b = \vartheta_b + \tau_b$, where $\iota_a \in I$, $\vartheta_b \in J$, and $\tau_a, \tau_b \in T$. Then

$$\bar{L}(b^* p a) = \langle [pa], [b] \rangle = \langle [\tau_a], [\tau_b] \rangle = L(\tau_b^* \tau_a) = L(b^* a),$$

since $L(\tau_b^* \iota_a) = L(\vartheta_b^* \tau_a) = L(\iota_b^* \vartheta_a) = 0$. Therefore \bar{L} is an extension of L . Further, \bar{L} is a flat extension since $\mathbb{R}\langle x, x^* \rangle \mathfrak{C} = I \oplus T$, and clearly $I = \{\theta \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C} \mid \bar{L}(\theta^* \theta) = 0\}$. Finally, as mentioned, any flat extension of L must satisfy $\bar{L}(p_m^* p_m) = 0$ for each monomial $m \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$, so by Lemma 5.1, we must have $\bar{L}(\mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}) = \{0\}$. Therefore, \bar{L} is unique since $\mathbb{R}\langle x, x^* \rangle \mathfrak{C} = I \oplus T$, and the value of \bar{L} on each of $T^* T$, $(I \oplus T)^* I$ and $I^* T$ is uniquely determined.

Finally, we extend \bar{L} to a flat extension on all of $\mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$ as follows. Lemma 2.3 implies that $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C}$ is equal to

$$\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C} = \bigoplus_{i,j \in \Gamma(\mathfrak{C})} E_{i,j} \otimes \mathbb{R} \langle x, x^* \rangle.$$

Extend \bar{L} to be 0 on the set

$$\bigoplus_{(k_1, k_2) \notin \Gamma(\mathfrak{C})^2} E_{k_1 k_2} \otimes \mathbb{R} \langle x, x^* \rangle.$$

Clearly this is a flat extension of L to all of $\mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$. \square

5.1. The GNS Construction. Proposition 5.3 below describes the well-known Gelfand-Naimark-Segal (GNS) construction.

Proposition 5.3. *Let L be a positive linear functional on $\mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$, and let $I = \{\vartheta \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle \mid L(\vartheta^* \vartheta) = 0\}$. There exists an inner product on the quotient space $\mathcal{H} := \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle / I$, a tuple of (possibly unbounded) operators X on \mathcal{H} , and a vector $v \in \mathcal{H}^n$ such that for each $p \in \mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$ we have*

$$\langle p(X)v, v \rangle = L(p).$$

and $\mathcal{H} = \{q(X)v \mid q \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle\}$.

Proof. Define an inner product on \mathcal{H} to be

$$\langle [p], [q] \rangle := L(q^* p).$$

This inner product is well defined since L is positive, and, by Lemma 5.1, is 0 on the space $\mathbb{R}^{1 \times \ell} I + I^* \mathbb{R}^{1 \times \ell}$. Let X be the tuple of operators on \mathcal{H} such that for each variable x_k , the operator X_k is defined by $X_k[p] := [x_k p]$. Since I is a left module by Lemma 5.1, X is well defined. Further,

$$\langle X_k^*[p], [q] \rangle = \langle [p], X_k[q] \rangle = \langle [p], [x_k q] \rangle = L(q^* x_k^* p) = \langle [x_k^* p], [q] \rangle.$$

Therefore $X_k^*[p] = [x_k^* p]$. Further, it follows that for any $r \in \mathbb{R} \langle x, x^* \rangle$ that $r(X)[p] = [rp]$.

Fix $v \in \mathcal{H}^\ell$ to be

$$v := \begin{pmatrix} [e_1 \otimes 1] \\ \vdots \\ [e_\ell \otimes 1] \end{pmatrix}.$$

If $q = \sum_{i=1}^\ell e_i \otimes q_i \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$, then

$$q(X)v = \sum_{i=1}^\ell q_i(X)[e_i \otimes 1] = \sum_{i=1}^\ell [e_i \otimes q_i] = [q].$$

Therefore,

$$\mathcal{H} = \{q(X)v \mid q \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle\}.$$

If $p = \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} E_{ij} \otimes p_{ij} \in \mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$, we see

$$p(X)v = \begin{pmatrix} \sum_{j=1}^{\ell} p_{1j}(X)[e_j \otimes 1] \\ \vdots \\ \sum_{j=1}^{\ell} p_{\ell j}(X)[e_j \otimes 1] \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{\ell} [e_j \otimes p_{1j}] \\ \vdots \\ \sum_{j=1}^{\ell} [e_j \otimes p_{\ell j}] \end{pmatrix}$$

so that

$$\begin{aligned} \langle p(X)v, v \rangle &= \sum_{i=1}^{\ell} \left\langle \sum_{j=1}^{\ell} [e_j \otimes p_{ij}], [e_i \otimes 1] \right\rangle \\ &= \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} L(E_{ij} \otimes p_{ij}) = L(p). \end{aligned}$$

□

Corollary 5.4. Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a finite right chip space. Let L be a positive linear functional on $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, and let J be the set

$$J := \{\vartheta \in \mathfrak{C} \mid L(\vartheta^* \vartheta) = 0\}.$$

Further, suppose there exists a positive extension of L to $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_2 \mathfrak{C}$.

Let $n := \dim(\mathfrak{C}) - \dim(J \cap \mathfrak{C})$, and suppose $n > 0$. There exists a tuple X of $n \times n$ matrices over \mathbb{R} and a vector $v \in \mathbb{R}^{\ell n}$ such that for each $p \in \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$ we have

$$v^* p(X) v = L(p).$$

and $\mathbb{R}^{\ell n} = \{p(X)v \mid p \in \mathfrak{C}\}.$

Proof. By Proposition 5.2, there exists a flat extension \bar{L} of L to all of $\mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$. Given this flat extension, apply Proposition 5.3 to produce the desired X and v . □

5.2. Non-Commutative Hankel Matrices. Let $\omega = (\omega_i)_{i=1}^k$ be a vector whose entries form a basis for a vector space $W \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$. Given a linear functional L on $W^* W$, the **non-commutative Hankel matrix for L (with respect to ω)** is the matrix $A = (L(\omega_i^* \omega_j))_{1 \leq i, j \leq k}$. This concept is a non-commutative analog of moment matrices—see [7], [8], for example.

Recall that \mathbb{S}^k is the set of $k \times k$ symmetric matrices over \mathbb{R} . Define $\langle A, B \rangle := \text{Tr}(AB)$ to be the inner product on \mathbb{S}^k .

Lemma 5.5. *Let $\omega = (\omega_i)_{i=1}^k$ be a vector whose entries form a basis for a vector space $W \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$. Let $A \in \mathbb{S}^k$ be a matrix. Let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a left module, and define \mathcal{Z} to be*

$$\mathcal{Z} := \{C \in \mathbb{S}^k \mid \omega^* C \omega \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}\}$$

Then A is the non-commutative Hankel matrix for some symmetric linear functional L on $W^ W$ such that $L([\mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}] \cap W^* W) = \{0\}$ if and only if $A \in \mathcal{Z}^\perp$, in which case*

$$(5.3) \quad L(\omega^* C \omega) = \text{Tr}(AC)$$

for each $C \in \mathbb{R}^{k \times k}$.

Proof. First, suppose $A = (a_{ij})_{1 \leq i, j \leq k}$ is the Hankel matrix of L and $L([\mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}] \cap W^* W) = \{0\}$. Then given $C = (c_{ij})_{1 \leq i, j \leq k}$,

$$L(\omega^* C \omega) = L\left(\sum_{i=1}^k \sum_{j=1}^k c_{ij} \omega_i^* \omega_j\right) = \sum_{i=1}^k \sum_{j=1}^k a_{ij} c_{ij} = \text{Tr}(AC).$$

It is therefore clear that $A \in \mathcal{Z}^\perp$.

Conversely, given $A = (a_{ij})_{1 \leq i, j \leq k} \in \mathcal{Z}^\perp$, (5.3) gives a well-defined linear functional since if $\omega^* C \omega = 0 \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}$, then $\text{Tr}(AC) = 0$. Further

$$L(\omega_i^* \omega_j) = L(\omega^* E_{ij} \omega) = \text{Tr}(A E_{ij}) = a_{ij}.$$

□

Proposition 5.6. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a finite right chip space. Let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a left module generated by polynomials in $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$. Let $\tau = (\tau_i)_{i=1}^k$ be a vector whose entries are all elements of $\text{Nlm}(I) \cap \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, and let T be the span of the τ_i . Let L be a symmetric linear functional on $T^* T$, and let $A \in \mathbb{S}^k$ be its non-commutative Hankel matrix. Let $\mathcal{Z} \subseteq \mathbb{S}^k$ be the space*

$$\{Z \in \mathbb{S}^k \mid \tau^* Z \tau \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}\}$$

Then L can be extended to a positive linear functional \bar{L} on $\mathfrak{C}^ \mathbb{R} \langle x, x^* \rangle_2 \mathfrak{C}$ such that*

- (1) $\bar{L}(\iota) = L(\iota^*) = 0$ for each $\iota \in \mathbb{R}^{\ell \times 1} I$
- (2) $\bar{L}(a^* a) = 0$ if and only if $a \in I$.

if and only if $A \succ 0$ and $A \in \mathcal{Z}^\perp$.

Proof. First, if there exists such a \bar{L} , then it is clear from (5.3) that $L(a^* a) > 0$ for each $a \in T$ if and only if $A \succ 0$, and further, Lemma 5.5 implies that $A \in \mathcal{Z}^\perp$.

Conversely, let $A \succ 0$ and $A \in \mathcal{Z}^\perp$. We see that $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_2 \mathfrak{C} = (\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C})^* (\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C})$, so it suffices to define \bar{L} on products $p_1^* p_2$,

where $p_1, p_2 \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$. If $\iota \in I \cap \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$ and $p \in \mathbb{R}\langle x, x^* \rangle_1$, define $\overline{L}(p^* \iota) = \overline{L}(\iota^* p) = 0$. This agrees with the definition of L by Lemma 5.5, and Lemma 4.2 implies that $\overline{L}(\theta) = \overline{L}(\theta^*) = 0$ for each $\theta \in \mathbb{R}^{\ell \times 1} I$ on which \overline{L} is defined. Further, if $a^* a \in \mathfrak{C}^* \mathbb{R}\langle x, x^* \rangle_2 \mathfrak{C}$, then Lemma 7.1 implies that each $a \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$. Hence $a = \iota + \beta^* \tau$, where $\iota \in \mathbb{R}_1^{\ell \times 1} I$ and $\beta \in \mathbb{R}^k$ is a constant vector. Since $A \succ 0$, by (5.3) we see that $\overline{L}(a^* a) = \beta^* A \beta = 0$ if and only if $\beta = 0$, which is equivalent to $a \in I$. \square

Lemma 5.7. *Let $\mathcal{B} \subseteq \mathbb{S}^k$ be a vector subspace. Then exactly one of the following holds:*

- (1) *There exists $B \in \mathcal{B}$ such that $B \succ 0$, and there exists no nonzero $A \in \mathcal{B}^\perp$ with $A \succeq 0$.*
- (2) *There exists $A \in \mathcal{B}^\perp$ such that $A \succ 0$, and there exists no nonzero $B \in \mathcal{B}$ with $B \succeq 0$.*
- (3) *There exist nonzero $B \in \mathcal{B}$ and $A \in \mathcal{B}^\perp$ with $A, B \succeq 0$, but there exist no $B \in \mathcal{B}$ nor $A \in \mathcal{B}^\perp$ with either $A \succ 0$ or $B \succ 0$.*

Proof. Let B_1, \dots, B_n be an orthonormal basis for \mathcal{B} , and let A_1, \dots, A_m be an orthonormal basis for \mathcal{B}^\perp . Define $L(\alpha, \beta)$, where $\alpha \in \mathbb{R}^m$ and $\beta \in \mathbb{R}^n$, to be

$$L(\alpha, \beta) := \sum_{i=1}^m \alpha_i A_i + \sum_{j=1}^n \beta_j B_j.$$

The elements of \mathcal{B} are precisely all matrices of the form $L(0, \beta)$ and the elements of \mathcal{B}^\perp are precisely all matrices of the form $L(\alpha, 0)$. For any pair (α, β) ,

$$\langle L(\alpha, 0), L(0, \beta) \rangle = 0.$$

If $L(\alpha, 0) \succ 0$ for some $\alpha \in \mathbb{R}^m$, then $L(0, \beta) \not\succeq 0$ for each $\beta \in \mathbb{R}^n \setminus \{0\}$. Similarly, if $L(0, \beta) \succ 0$ for some $\beta \in \mathbb{R}^n$, then $L(\alpha, 0) \not\succeq 0$ for each $\alpha \in \mathbb{R}^m \setminus \{0\}$. Therefore, either (1) or (2) holds, or there exist no $B \in \mathcal{B}$ nor $A \in \mathcal{B}^\perp$ with either $A \succ 0$ or $B \succ 0$.

Assume that (1) and (2) do not hold. Let $\mathcal{C} \subseteq \mathbb{R}^n$ be the set

$$\mathcal{C} = \{\beta \in \mathbb{R}^n \mid \text{exists } \alpha \in \mathbb{R}^m \text{ such that } L(\alpha, \beta) \succ 0\}.$$

Since L is onto and linear, \mathcal{C} is nonempty and convex. If $0 \in \mathcal{C}$, then $L(\alpha, 0) \succ 0$ for some α , which is a contradiction. Therefore, $0 \notin \mathcal{C}$, which implies that there exists $x \in \mathbb{R}^n \setminus \{0\}$ such that $\langle x, \beta \rangle \geq 0$ for all $\beta \in \mathcal{C}$. Therefore, for each positive-definite matrix, which, since L is onto, must be of the form $L(\alpha, \beta) \succ 0$,

$$\langle L(0, x), L(\alpha, \beta) \rangle = \langle x, \beta \rangle \geq 0,$$

which implies that $L(0, x) \succeq 0$. Similarly, there exists $\alpha \in \mathbb{R}^m \setminus \{0\}$ such that $L(\alpha, 0) \succeq 0$. \square

We now use Lemma 5.7 to construct positive linear functionals.

Lemma 5.8. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a finite right chip space and let $I \subseteq \mathbb{R} \langle x, x^* \rangle^{1 \times \ell}$ be a real left module generated by polynomials in $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$. There exists a positive linear functional L on $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_2 \mathfrak{C}$ such that the following hold:*

- (1) $L(a^* a) > 0$ for each $a \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus I$
- (2) $L(\iota) = 0$ for each $\iota \in (\mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}) \cap \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_2 \mathfrak{C}$.

Proof. Let $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} = I \oplus T$ for some space T . Let τ be a vector of length μ whose entries form a basis for T . Let $\mathcal{Z} \subseteq \mathbb{S}^\mu$ be defined by

$$\mathcal{Z} := \{Z \mid \tau^* Z \tau \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}\}.$$

Since I is real, the space \mathcal{Z} contains no $Z \neq 0$ with $Z \succeq 0$. By Lemma 5.7 there exists a positive-definite matrix $C \in \widehat{\mathcal{Z}}^\perp$. By Lemma 5.5, there exists a positive linear functional L on $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_2 \mathfrak{C}$ which gives the result. \square

Lemma 5.9. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a finite right chip space and let $I \subsetneq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a real left module generated by polynomials in $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$. Let $n = \dim(\mathfrak{C}) - \dim(I \cap \mathfrak{C})$. There exists $(X, v) \in V(I)^{(n)}$ such that $p(X)v \neq 0$ if $p \in \mathfrak{C} \setminus I$.*

Proof. First, $I \neq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ implies that $n > 0$. Let L be a linear functional with the properties described by Lemma 5.8. We see that L restricts to a functional on $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$. By Corollary 5.4 we produce a tuple $(X, v) \in (\mathbb{R}^{n \times n})^g \times \mathbb{R}^n$, for some $n \in \mathbb{N}$, such that $v^* p(X) v = L(p)$ for each $p \in \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, and such that

$$\mathbb{R}^n = \{c(X)v \mid c \in \mathfrak{C}\}.$$

Therefore if $a \in \mathfrak{C}$,

$$\|a(X)v\|^2 = v^* a(X)^* a(X) v = L(a^* a)$$

which is nonzero if and only if $a \notin I$. Further, if $\iota \in I \cap \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, then $L(c^* \iota) = 0$ for each $c \in \mathfrak{C}$ by Proposition 5.2. Since $\iota(X)v \in \mathbb{R}^n$, there exists some $c \in \mathfrak{C}$ such that $c(X)v = \iota(X)v$ and so

$$\|\iota(X)v\|^2 = v^* c^*(X) \iota(X) v = L(c^* \iota) = 0.$$

Since I is generated by its elements in $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, this implies that $(X, v) \in V(I)$. \square

5.3. The Matrix Non-Commutative Left Nullstellensatz.

Proposition 5.10. *If $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ is a finitely-generated left module, then $\sqrt[r]{I} = \sqrt{I}$.*

Proof. Let $p \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$. Choose d sufficiently large so that $\deg(p) \leq d$ and so that I is generated by polynomials with degree bounded by d . Let $\mathfrak{C} = \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle_d$. Then Lemma 5.9 implies the existence of a tuple $(X, v) \in V(I)$ such that $p(X)v \neq 0$. \square

We now prove Theorem 1.3.

Proof of Theorem 1.3. Note that $p_i(X)v = 0$ means each row of $p_i(X)v = 0$, i.e. $e_k^* p_i(X)v = 0$ for each $e_k \in \mathbb{R}^{1 \times \nu_i}$. Therefore

$$V(I) = V \left(\sum_{i=1}^k \mathbb{R}^{1 \times \nu_i} \langle x, x^* \rangle p_i \right).$$

The first part of the result follows from Proposition 5.10.

Next, if q is an element of the real left module (1.2), then

$$q = \sum_i^{\text{finite}} \sum_{j=1}^k a_{ij} b_{ij} p_j$$

for some $a_{ij} \in \mathbb{R}^{\nu \times 1}$ and $b_{ij} \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$. Therefore,

$$q = \left(\sum_i^{\text{finite}} a_{ij} b_{ij} \right) p_j.$$

\square

6. EXTENSION TO \mathbb{C} AND \mathbb{H}

We now show how to extend the main results of the paper to the case where the polynomials have complex or quaternion coefficients.

There are well-known injective homomorphisms of \mathbb{C} and \mathbb{H} into $\mathbb{R}^{2 \times 2}$ and $\mathbb{R}^{4 \times 4}$ respectively. It therefore makes sense to think of matrices of NC polynomials in with coefficients in \mathbb{C} or \mathbb{H} as matrices of NC polynomials with coefficients in \mathbb{R} .

Let $\mathbb{C} \langle x, x^* \rangle$ be the space of NC polynomials with coefficients in \mathbb{C} . Here, the involution $*$ acts on \mathbb{C} by conjugation so that for each $p \in \mathbb{C} \langle x, x^* \rangle$ we have $p^*(X) = p(X)^*$, where $*$ on complex matrices denotes the conjugate transpose.

Let $\mathbb{H} \langle x, x^* \rangle$ denote the space of NC polynomials over \mathbb{H} . Here the letters x_i and x_j^* do not commute with the non-real elements of \mathbb{H} because, in general, if $a \in \mathbb{H} \setminus \mathbb{R}$ and $X \in \mathbb{H}^{n \times n}$, then $aX \neq Xa$.

We also define a space $\mathbb{H}_c\langle z, z^* \rangle$ to be the space of NC polynomials over \mathbb{H} where the letters z_i and z_j^* commute with \mathbb{H} .

Over these spaces, there are precise analogs of left module, zero set, radical left module, and real left module, which will be denoted as they were in the real case.

6.1. Quaternion Case. The most general case $\mathbb{H}\langle x, x^* \rangle$. We now present some simple results for that case, noting that the complex valued case is similar (but slightly easier).

Let $\psi : \mathbb{H} \rightarrow \mathbb{R}^{1 \times 4}$ be the \mathbb{R} -linear bijection defined by

$$\psi(a + bi + cj + dk) = (a, b, c, d).$$

We further extend ψ to $\mathbb{H}^{\nu \times \ell}$ by coordinates. Further, we can extend ψ to map $\mathbb{H}_c^{\nu \times \ell}\langle z, z^* \rangle$ into $\mathbb{R}^{4\nu \times 4\ell}\langle x, x^* \rangle$ by applying ψ to coefficients and replacing $\langle z, z^* \rangle$ with $\langle x, x^* \rangle$. This extension of ψ is $\mathbb{R}\langle x, x^* \rangle$ -linear.

Proposition 6.1. *If $I \subseteq \mathbb{H}_c^{1 \times \ell}\langle x, x^* \rangle$ is a left module, then $J = \psi(I) \subseteq \mathbb{R}^{1 \times 4\ell}\langle x, x^* \rangle$ is also a left module. Further, I is real if and only if J is.*

Proof. If $a, b \in I$, then clearly $\psi(a) + \psi(b) = \psi(a + b) \in J$ since ψ is linear. Further, if $c \in \mathbb{R}\langle x, x^* \rangle$, then $c\psi(a) = \psi(ca) \in J$. Therefore J is a left module.

It is an easy exercise to show that I being real implies that J is real. Conversely, suppose

$$\sum_i^{\text{finite}} p_i^* p_i = \sum_j^{\text{finite}} q_j^* r_j + \sum_j^{\text{finite}} r_j^* q_j$$

where each $p_i, q_j, r_j \in \mathbb{H}_c^{1 \times \ell}\langle z, z^* \rangle$, and $r_j \in I$. Let $\phi : \mathbb{H} \rightarrow \mathbb{R}^{4 \times 4}$ be the injective homomorphism

$$\phi(a + bi + cj + dk) = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & c & b & a \end{pmatrix} = \begin{pmatrix} \psi(a + bi + cj + dk) \\ \psi(i(a + bi + cj + dk)) \\ \psi(j(a + bi + cj + dk)) \\ \psi(k(a + bi + cj + dk)) \end{pmatrix}$$

and extend ϕ to $\mathbb{H}_c^{1 \times \ell}\langle z, z^* \rangle$ by coordinates. Then

$$\sum_i^{\text{finite}} \phi(p_i)^* \phi(p_i) = \sum_j^{\text{finite}} \phi(q_j)^* \phi(r_j) + \sum_j^{\text{finite}} \phi(r_j)^* \phi(q_j).$$

The rows of each $\phi(r_j)$ are $\psi(r_j), \psi(ir_j), \psi(jr_j), \psi(kr_j) \in J$. Therefore, if J is real, then each row of each $\phi(p_i)$ is in J . In particular, $\psi(p_i)$ is a row of $\phi(p_i)$, so each $p_i \in I$. \square

If $x = (x_1, \dots, x_g)$ and $z = (z_1, \dots, z_{4g})$, define a map $\varphi : \mathbb{H}\langle x, x^* \rangle \rightarrow \mathbb{H}_c\langle z, z^* \rangle$ by

$$\varphi(p) = p(z_1 + iz_2 + jz_3 + kz_4, \dots, z_{4g-3} + iz_{4g-2} + jz_{4g-1} + kz_{4g}).$$

Clearly φ is an injective homomorphism. Further, we see that φ is actually surjective and has inverse given by the maps

$$\begin{aligned} z_{4m-3} &\mapsto \frac{1}{4}(x_m - ix_m i - jx_m j - kx_m k) \\ z_{4m-2} &\mapsto \frac{1}{4}(-ix_m - x_m i - kx_m j + jx_m k) \\ z_{4m-1} &\mapsto \frac{1}{4}(-jx_m + kx_m i - x_m j - ix_m k) \\ z_{4m} &\mapsto \frac{1}{4}(-kx_m - jx_m i + ix_m j - x_m k) \end{aligned}$$

Proposition 6.2. *Let $I \subseteq \mathbb{H}\langle x, x^* \rangle$ be a subset and let $J = \varphi(I)$. Then I is a left module if and only if J is. Further, if I and J are left modules, I is real if and only if J is.*

Proof. This follows easily from φ being a bijective homomorphism between $\mathbb{H}\langle x, x^* \rangle$ and $\mathbb{H}_c\langle z, z^* \rangle$. \square

6.2. Extension of the Left Nullstellensatz to \mathbb{C} and \mathbb{H} .

Corollary 6.3. Let $\mathbb{F} = \mathbb{R}, \mathbb{C}$ or \mathbb{H} . Let p_1, \dots, p_k be such that each $p_i \in \mathbb{F}^{\nu_i \times \ell}\langle x, x^* \rangle$ for some $\nu_i \in \mathbb{N}$. Define

$$J_\nu := \mathbb{F}^{\nu \times 1} \sqrt[k]{\sum_{i=1}^k \mathbb{F}^{1 \times \nu_i} \langle x, x^* \rangle p_i}$$

for $\nu \in \mathbb{N}$. Let $q \in \mathbb{F}^{\nu \times \ell}\langle x, x^* \rangle$. Then $q(X)v = 0$ for all $(X, v) \in \bigcup_{n \in \mathbb{N}} (\mathbb{F}^{n \times n})^g \times \mathbb{F}^{\ell n}$ such that $p_1(X)v, \dots, p_k(X)v = 0$ if and only if $q \in J_\nu$.

Proof. The \mathbb{R} case is Theorem 1.3. As we saw in that case, this result boils down to showing $\sqrt{I} = \sqrt[k]{I}$ for any finitely-generated left module $I \subseteq \mathbb{F}^{1 \times \ell}\langle x, x^* \rangle$. We will do the $\mathbb{F} = \mathbb{H}$ case here; the \mathbb{C} case is similar but easier.

Let $q \notin \sqrt[k]{I}$. It suffices to show that $q \notin \sqrt{I}$. We see that $\psi \circ \varphi(q) \notin \psi \circ \varphi(\sqrt[k]{I})$. Propositions 6.1 and 6.2 imply that $\psi \circ \varphi(\sqrt[k]{I})$ is real, so

$$\psi \circ \varphi(I) \subseteq \sqrt{\psi \circ \varphi(I)} \subseteq \psi \circ \varphi(\sqrt[k]{I})$$

which implies that $\psi \circ \varphi(q) \notin \sqrt{\psi \circ \varphi(I)}$. Proposition 5.10 implies that there exists a real tuple $(Z, v) \in V(\psi(I))$ such that $\psi \circ \varphi(q)(Z)v \neq 0$.

Express $\varphi(q)$ as

$$\varphi(q) = (q_1 + iq_2 + jq_3 + kq_4, \dots, q_{4\ell-3} + iq_{4\ell-2} + jq_{4\ell-1} + kq_{4\ell}).$$

Then,

$$(\psi(q_1)(Z), \dots, \psi(q_{4\ell})(Z)) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_{4\ell} \end{pmatrix} = \sum_{i=1}^{4\ell} \psi(q_i)(Z)v_i \neq 0.$$

Let $w \in \mathbb{H}^\ell$ be

$$w = \begin{pmatrix} v_1 - iv_2 - jv_3 - kv_4 \\ \vdots \\ v_{4\ell-3} - iv_{4\ell-2} - jv_{4\ell-1} - kv_{4\ell} \end{pmatrix}$$

and let $X \in (\mathbb{H}^{n \times n})^g$ be

$$X = (Z_1 + iZ_2 + jZ_3 + kZ_4, \dots, Z_{4g-3} + iZ_{4g-2} + jZ_{4g-1} + kZ_{4g}).$$

If $r \in \mathbb{H}^{1 \times \ell} \langle x, x^* \rangle$, then

$$r(X) = \varphi(r)(Z),$$

and further, it is easy to show that

$$\operatorname{Re}(\varphi(r)(Z)w) = \psi \circ \varphi(r)(Z)v.$$

Therefore

$$\operatorname{Re}(q(X)w) = \psi \circ \varphi(q)(X)v \neq 0.$$

Also, if $p \in \sqrt[\ell]{I}$, then for each $a \in \mathbb{H}$,

$$\operatorname{Re}(ap(X)w) = \psi \circ \varphi(ap)(X)v = 0,$$

which implies that $p(X)w = 0$. Therefore $(X, w) \in V(I)$, which shows that $q \notin \sqrt{I}$. \square

Note that a Corollary of this result is an extension of [5, Theorem 1.6] to \mathbb{H} .

7. THE REAL RADICAL OF A LEFT MODULE IN $\mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$

We now use the results of Sections 3 and 4 to prove a strong result, Theorem 7.3, about the real radical of a finitely-generated left ideal. This result is both a generalization of and an improvement upon [5, Corollary 2.6]. We prepare for the proof of Theorem 7.3 with several lemmas.

Lemma 7.1. *Let \prec_0 be a degree order on $\langle x, x^* \rangle$ such if $a = a_1a_2$, $b = b_1b_2$, where $|a_1| = |a_2| = |b_1| = |b_2| = d$ for some degree d , then $a \prec_0 b$ if one of the following holds:*

- (1) $a_2 \prec_0 b_2$, or
- (2) $a_2 = b_2$ and $a_1 \prec_0 b_1$.

Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a right chip space, and let $\prec_{\mathfrak{C}}$ be a \mathfrak{C} -order induced by \prec_0 , and let $\prec_{\mathfrak{C} \times \mathfrak{C}}$ be a double \mathfrak{C} -order induced by $\prec_{\mathfrak{C}}$. Let $p \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$. Then the leading monomial of p^*p is $\text{lm}(p)^* \text{lm}(p)$, where $\text{lm}(p)$ is the leading monomial of p . Further, $\text{lm}(p)^* \text{lm}(p)$ has a positive coefficient in p^*p .

Proof. Let p be decomposed as

$$p = \sum_{w \in \langle x, x^* \rangle} \sum_{m \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}} A(w, m)wm + \bar{p},$$

where $A(w, m) \in \mathbb{R}$ and $\bar{p} \in \mathfrak{C}$. Since $p \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$ by assumption, at least some of the $A(w, m)$ are nonzero. Let d be the maximum length of any w such that $A(w, m) \neq 0$ for any m .

For any $m_1, m_2 \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$ and $w_1, w_2 \in \langle x, x^* \rangle$ the representation $(w_1 m_1)^* (w_2 m_2) = m_1^* (w_1^* w_2) m_2$ is the unique representation given by Lemma 2.8 with left and right factors being in $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$.

If $c \in \mathfrak{C}$, $m \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$, and $|w| \leq d$, then either $m^* w^* c$ and $c^* w m$ are in $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$, or $m^* w^* c = m^* w_2^* (w_1^* c)$ and $c^* w m = (w_1^* c)^* w_2 m$, where $w = w_1 w_2$ and $w_1^* c \in \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}$, with $|w_1| < |w|$. Therefore, the terms of p^*p in $\mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle \mathfrak{C} \setminus \mathfrak{C}^* \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$ whose representation given by Lemma 2.8 has a middle word of maximum length are those of the form $m_1^* w_1^* w_2 m_2$ with $m_1, m_2 \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ and $|w_1| = |w_2| = d$. Each such term of p is uniquely a product of $(w_1 m_1)^*$ and $w_2 m_2$ since d is the maximum length of the leftmost word w_1 and w_2 in p .

In p^*p , the monomial $m_1^* w_1^* w_2 m_2$ has coefficient $A(w_1, m_1)A(w_2, m_2)$, and hence is nonzero if and only if both $A(w_1, m_1)$ and $A(w_2, m_2)$ are nonzero. Let $w_* m_* = \text{lm}(p)$ be the leading monomial of p . If $A(w_1, m_1), A(w_2, m_2) \neq 0$, we have $w_1 m_1, w_2 m_2 \preceq_{\mathfrak{C}} w_* m_*$. Then clearly $m_1^* w_1^* w_2 m_2 \prec_{\mathfrak{C} \times \mathfrak{C}} m_*^* w_*^* w_* m_*$. Therefore, the leading monomial of p^*p is $\text{lm}(p)^* \text{lm}(p)$. Further, the coefficient of $\text{lm}(p)^* \text{lm}(p)$ is $A(m_* w_*)^2 > 0$. \square

Lemma 7.2. Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a finite right chip space. Let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a left module generated by polynomials in $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$. If

$$(7.1) \quad \sum_i^{\text{finite}} p_i^* p_i \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell},$$

for some $p_i \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$, then each $p_i \in I + \mathfrak{C}$.

Proof. Suppose (7.1) holds. Let Θ be the space

$$\Theta = \sum_{j \notin \Gamma(\mathfrak{C})} e_j \otimes \mathbb{R}\langle x, x^* \rangle,$$

so that, by Lemma 2.2, $\mathbb{R}^{1 \times \ell} \langle x, x^* \rangle = \mathbb{R}\langle x, x^* \rangle \mathfrak{C} \oplus \Theta$. Let $p_i = c_i + \theta_i$ for each i , where $c_i \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C}$ and $\theta_i \in \Theta$. We see that

$$\sum_i^{\text{finite}} p_i^* p_i = \sum_i^{\text{finite}} c_i^* c_i + \sum_i^{\text{finite}} c_i^* \theta_i + \sum_i^{\text{finite}} \theta_i^* c_i + \sum_i^{\text{finite}} \theta_i^* \theta_i.$$

Since (2.1) holds and $I \subseteq \mathfrak{C}$, it must be that $\sum_i \theta_i^* \theta_i = 0$, which can only occur if each $\theta_i = 0$. Therefore each $p_i \in \mathbb{R}\langle x, x^* \rangle \mathfrak{C}$.

Given a polynomial p_i , either $p_i \in \mathfrak{C}$ or $p_i \in \mathbb{R}\langle x, x^* \rangle \setminus \mathfrak{C}$ and, by Lemma 7.1, $\text{lm}(p_i^* p_i) = \text{lm}(p_i)^* \text{lm}(p_i)$. In the latter case, the leading monomial of $\sum_i p_i^* p_i$ must be the maximal $\text{lm}(p_i)^* \text{lm}(p_i)$ since the leading monomials of the $p_i^* p_i$, with $p_i \notin \mathfrak{C}$, cannot cancel each other because by Lemma 7.1 they all have positive coefficients. Let p_{i_*} such that $\text{lm}(p_{i_*})$ is maximal. By Lemma 4.2, the leading monomial $\text{lm}(p_{i_*})^* \text{lm}(p_{i_*})$ is of the form $m^* \text{lm}(\iota)$ or $\text{lm}(\iota)^* m$, for some $\iota \in I \cap \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ and $m \in \mathbb{R}\langle x, x^* \rangle \setminus \mathfrak{C}$. Since $\text{lm}(p_{i_*}) \notin \mathfrak{C}$, decompose $\text{lm}(p_{i_*})$ by Lemma 2.7 as $u\bar{p}$, where $u \in \langle x, x^* \rangle$ and $\bar{p} \in \mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$. By Lemma 2.5, we must have $\bar{p} = \text{lm}(\iota)$. Let A be the coefficient of $\text{lm}(p_{i_*})$ in p_{i_*} . Then

$$\sum_{i \neq i_*} p_i^* p_i + (p_{i_*} - A u \iota)^* (p_{i_*} - A u \iota) \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell},$$

and further, $p_{i_*} - A u \iota$ has a smaller leading monomial than p_{i_*} does, and $p_{i_*} \in I + \mathfrak{C}$ if and only if $p_{i_*} - A u \iota \in I + \mathfrak{C}$.

We repeat this process inductively to show that each $p_i \in I + \mathfrak{C}$. \square

The following theorem is a key result in computing the real radical of a finitely-generated left module. This result is a generalization of [5, Corollary 2.6] to $\mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$. Further, the following result gives is more refined than [5, Corollary 2.6] for verifying whether or not a left module is real.

Theorem 7.3. *Let $\mathfrak{C} \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a finite right chip space, and let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a left module generated by polynomials in $\mathbb{R}\langle x, x^* \rangle_1 \mathfrak{C}$. Let $(\{\iota_i\}_{i=1}^\mu, \{\vartheta_j\}_{j=1}^\sigma)$ be a \mathfrak{C} -basis for I . Then I is real if and only if whenever*

$$(7.2) \quad \sum_i^{\text{finite}} p_i^* p_i = \sum_{j=1}^\mu (q_j \iota_j + \iota_j^* q_j^*) + \sum_{k=1}^\sigma (\alpha_k^* \vartheta_k + \vartheta_k^* \alpha_k),$$

for some $p_i, q_j \in \mathfrak{C}$ and $\alpha_k \in \mathbb{R}^{1 \times \ell} \cap \mathfrak{C}$, then each $p_i \in I$.

Note that Theorem 7.3 implies that to test whether a left module $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ is real, given that I is generated by polynomials in $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$ for some right chip space \mathfrak{C} , one needs only verify whether given some polynomials $p_i \in \mathfrak{C}$ such that

$$\sum_i^{\text{finite}} p_i^* p_i \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}$$

if each p_i must be in I .

Proof. Suppose

$$\sum_i^{\text{finite}} p_i^* p_i \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell}.$$

Lemma 7.2 implies that each p_i is of the form $p_i = \phi_i + \psi_i$, where $\phi_i \in I$ and $\psi_i \in \mathfrak{C}$. Therefore

$$\sum_i^{\text{finite}} \psi_i^* \psi_i \in \mathbb{R}^{\ell \times 1} I + I^* \mathbb{R}^{1 \times \ell},$$

and so I is real if and only if we must have each $\psi_i \in I$. We get the righthand side of (7.2) from Lemma 4.2 (3), noting that a sum of squares is necessarily symmetric. \square

Note that Theorem 7.3 implies degree bounds. For example, if $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ is generated by polynomials of degree bounded by d , one could use $\mathfrak{C} = \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle_{d-1}$. However, Theorem 7.3 is more refined since in many cases there exists a smaller right chip space \mathfrak{C} such that I is generated by polynomials in $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$.

8. LEFT GRÖBNER BASES

Classically, Gröbner bases are used to verify whether a given polynomial p belongs to a given ideal I . We need left Gröbner bases for verifying membership in left modules $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$; specifically, we will need them for the Real Radical Algorithm in § 9.

Fortunately, there is a general theory of one-sided Gröbner bases for one-sided modules with coherent bases over algebras with ordered multiplicative basis [11]. In this section, we give a version of this theory specific to our case and tie it in with the \mathfrak{C} -basis theory previously presented. Left Gröbner bases are easily computable and are used to algorithmically determine membership in a left module.

A **left admissible order** \prec on $\langle x, x^* \rangle$ is a well order on $\langle x, x^* \rangle$ such that $a \prec b$ for some $a, b \in \langle x, x^* \rangle$ implies that for each $c \in \langle x, x^* \rangle$ we

have $ca \prec cb$. Given a left module $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$, a subset $\mathcal{G} \subseteq I$ is a **left Gröbner basis of I with respect to \prec** if the left module generated by $\text{lm}(\mathcal{G})$ equals the left module generated by $\text{lm}(I)$. We say a polynomial p is **monic** if the coefficient of $\text{lm}(p)$ in p is 1. We say a left Gröbner basis \mathcal{G} is **reduced** if the following hold:

- (1) Every element of \mathcal{G} is monic.
- (2) If $\iota_1, \iota_2 \in \mathcal{G}$, then $\text{lm}(\iota_1)$ does not divide any of the terms of ι_2 on the right.

Proposition 8.1. *Let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a left module and let \prec be a left admissible order. Then*

- (1) *There is a left Gröbner basis for I with respect to \prec .*
- (2) *There is a unique reduced left Gröbner basis for I with respect to \prec .*
- (3) *If \mathcal{G} is a left Gröbner basis for I with respect to \prec , then \mathcal{G} generates I as a left module.*
- (4) $\mathbb{R}^{1 \times \ell} = I \oplus \text{Span}(\text{Nlm}(I))$.

Proof. See [11, Propositions 4.2, 4.4]. □

Lemma 8.2. *Let $I \subseteq \mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle$ be a left module and let $\{\iota_i\}_{i \in \alpha}$ be a left Gröbner basis for I . Every element $p \in I$ can be expressed uniquely as*

$$(8.1) \quad p = \sum_i^{\text{finite}} q_i \iota_i,$$

for some $q_i \in \mathbb{R} \langle x, x^* \rangle$. In particular, the leading monomial of p is divisible on the right by the leading monomial of one of the left Gröbner basis elements ι_i .

Proof. Since $\{\iota_i\}_{i \in \alpha}$ generates I , every element $p \in I$ can be expressed as (8.1). Consider the leading monomial of such a p . If a is a monomial such that $a \prec \text{lm}(\iota_i)$, then for each $r \in \langle x, x^* \rangle$, we have $ra \prec r \text{lm}(\iota_i)$. Therefore the leading monomial of each $q_i \iota_i$ is of the form $\tilde{q}_i \text{lm}(\iota_i)$, where $\tilde{q}_i \in \langle x, x^* \rangle$ is some monomial appearing in q_i .

Suppose $\tilde{q}_i \text{lm}(\iota_i) = \tilde{q}_j \text{lm}(\iota_j) \neq 0$ for some $i \neq j$, and suppose $|\text{lm}(\iota_i)| \leq |\text{lm}(\iota_j)|$. If $\text{lm}(\iota_i) = E_{a_i b_i} \otimes w_i$ and $\text{lm}(\iota_j) = E_{a_j b_j} \otimes w_j$ for some $E_{a_i b_i}, E_{a_j b_j} \in \mathbb{R}^{\nu \times \ell}$ and $w_i, w_j \in \langle x, x^* \rangle$, then $E_{a_i b_i} \otimes \tilde{q}_i w_i = E_{a_j b_j} \otimes \tilde{q}_j w_j$. Therefore $a_i = a_j$, $b_i = b_j$, and $\tilde{q}_i w_i = \tilde{q}_j w_j$, with $|w_i| \leq |w_j|$. This implies that $\text{lm}(\iota_i)$ divides $\text{lm}(\iota_j)$ on the right, which contradicts the properties of the left Gröbner basis. Therefore the leading monomials of the nonzero $q_i \iota_i$ are all distinct, which implies by Lemma 3.1, that either each $q_j = 0$, or the leading monomial of p is the

maximal nonzero $\tilde{q}_i \text{lm}(\iota_i)$. Further, uniqueness follows from linearity and from Lemma 3.1. \square

8.1. Algorithm for Computing Reduced Left Gröbner Bases.

Let \prec be a left monomial order on $\mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle$. Let I be the left module generated by polynomials $\iota_1, \dots, \iota_\mu \in \mathbb{R}^{\nu \times \ell} \langle x, x^* \rangle$. It is easy to show that inputting $\iota_1, \dots, \iota_\mu$ into the following algorithm computes a reduced left Gröbner basis for I .

8.1.1. Reduced Left Gröbner Basis Algorithm.

- (1) Given: $\mathcal{G} = \{\iota_1, \dots, \iota_\mu\}$.
- (2) If $0 \in \mathcal{G}$, remove it. Further, perform scalar multiplication so that each element of \mathcal{G} is monic.
- (3) For each $\iota_i, \iota_j \in \mathcal{G}$, compare $\text{lm}(\iota_i)$ with the terms of ι_j .
 - (a) If $\text{lm}(\iota_i)$ divides a term of ι_j on the right, let $q \in \langle x, x^* \rangle$ and $\xi \in \mathbb{R}$ be such that $\xi q \text{lm}(\iota_i)$ is a term in ι_j . Replace ι_j with $\iota_j - \xi q \iota_i$. Repeat (2).
 - (b) If $\text{lm}(\iota_i)$ does not divide any terms of any ι_j on the right for any $i \neq j$, stop and output \mathcal{G} .

8.2. Reduced Left Gröbner Bases are \mathfrak{C} -Bases. For a well-chosen \mathfrak{C} and $\prec_{\mathfrak{C}}$, a reduced left Gröbner basis is actually a \mathfrak{C} -basis.

Proposition 8.3. *Let $I \subseteq \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$ be a finitely-generated left module with reduced left Gröbner basis $\iota_1, \dots, \iota_\mu$ according to some left monomial order \prec on $\mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$. Let \mathfrak{C} be the right chip space defined by*

$$\mathfrak{C} := \text{Span}(\{m \in \mathbb{R}^{1 \times \ell} \langle x, x^* \rangle \mid m \text{ proper right chip of a term of some } \iota_i\}),$$

and let $\prec_{\mathfrak{C}}$ be a \mathfrak{C} -order induced by \prec . Then $(\{\iota_i\}_{i=1}^\mu, \emptyset)$ is a \mathfrak{C} -basis.

Not that this algorithm outputs a basis with at most μ elements whose degree is no greater than the inputted elements, that the and that the algorithm is guaranteed to terminate in finite time.

Proof. First, $\iota_1, \dots, \iota_\mu \in \mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C}$ by construction. Next, each leading monomial $\text{lm}(\iota_i)$ must be in $\mathbb{R} \langle x, x^* \rangle_1 \mathfrak{C} \setminus \mathfrak{C}$ since otherwise $\text{lm}(\iota_i) \in \mathfrak{C}$, which implies that it properly divides a term of some other ι_j . By Lemma 8.2, the left Gröbner basis satisfies the conditions of Lemma 3.4 to be a \mathfrak{C} -basis. \square

A reduced left Gröbner basis is a nice \mathfrak{C} -basis since it has no elements of \mathfrak{C} in it.

9. THE REAL RADICAL ALGORITHM

In some simple cases, as shown in [4], it is easy to verify whether a left module is real. In general, however, an algorithmic approach is needed. In [5], a Real Radical Algorithm is presented for computing the real radical of any finitely-generated left ideal $J \subseteq \mathbb{R}\langle x, x^* \rangle$. We now present a new Real Radical Algorithm which extends the previous Real Radical Algorithm to finitely-generated left modules $I \subseteq \mathbb{R}^{1 \times \ell}\langle x, x^* \rangle$. Further, using right chip spaces, the new Real Radical Algorithm is much more efficient.

Let $I \subseteq \mathbb{R}^{1 \times \ell}\langle x, x^* \rangle$ be the left module generated by polynomials $\iota_1, \dots, \iota_\mu$. When $\{\iota_1, \dots, \iota_\mu\}$ is inputted into the following algorithm, the result is a reduced left Gröbner basis for $\sqrt[r]{I}$.

9.1. The Real Radical Algorithm.

- (1) Given: $\mathcal{G} = \{\iota_1, \dots, \iota_\mu\}$.
- (2) Fix a degree lexicographic order on $\mathbb{R}^{1 \times \ell}\langle x, x^* \rangle$. Compute a reduced left Gröbner basis from \mathcal{G} , and set $\mathcal{G}^{(0)}$ to be the resulting basis.
- (3) Let $i = 0$.
- (4) If $\mathcal{G}^{(i)}$ only contains constants, then stop and output $\mathcal{G}^{(i)}$.
- (5) Let $\mathfrak{C}^{(i)}$ be the set of monomials which properly divide a term of any of the polynomials in $\mathcal{G}^{(i)}$ on the right.
- (6) For each $\vartheta_j \in \mathcal{G}^{(i)}$, let q_j be the polynomial

$$q_j = \sum_{m \in \mathfrak{C}^{(i)}} \alpha_{m,j}^{(i)} m$$

where the $\alpha_{m,j}^{(i)}$ are real-valued variables, and test whether or not the polynomial

$$(9.1) \quad \sum_{\vartheta_j \in \mathcal{G}^{(i)}} q_j^* \vartheta_j + \vartheta_j^* q_j$$

is a nonzero sum of squares for some values of $\alpha_{m,j}^{(i)} \in \mathbb{R}$. See [18] for more on how to verify if a NC polynomial is a sum of squares, and see [17] and [2] for a computer algebra package which will do this. Our problem is more complicated than a standard sums of squares problem since we are dealing with a polynomial with variable coefficients. Therefore, we now spell out the details of a sum of squares algorithm.

SOS Algorithm

- (a) Given: (9.1).

- (b) For each monomial in (9.1) which is not in $(\mathfrak{C}^{(i)})^*(\mathfrak{C}^{(i)})$, set the coefficient equal to 0. Solve the resulting set of linear equations in terms of the $\alpha_{m,j}^{(i)}$ and reduce (9.1) to have only terms in $(\mathfrak{C}^{(i)})^*(\mathfrak{C}^{(i)})$.
- (c) Let M_i be a vector whose entries are all monomials in $\mathfrak{C}^{(i)}$. If desired, technically we can pick a smaller vector M_i by eliminating monomials of small degree. (See [18]).
- (d) Let $\mathcal{Z}^{(i)}$ be space

$$\mathcal{Z}^{(i)} = \{Z \text{ a real symmetric matrix} \mid M_i^* Z M_i = 0\},$$

and let $Z_1^{(i)}, \dots, Z_{n^{(i)}}^{(i)}$ be a basis for $\mathcal{Z}^{(i)}$.

- (e) For each $m^* \vartheta_j + \vartheta_j^* m$, let $B_{m,j}^{(i)}$ be a symmetric matrix such that

$$m^* \vartheta_j + \vartheta_j^* m = M_i^* B_{m,j}^{(i)} M_i.$$

- (f) In the linear pencil

$$(9.2) \quad L_i(\alpha^{(i)}, \beta^{(i)}) = \sum_{m \in \mathfrak{C}^{(i)}} \sum_{\vartheta_j \in \mathcal{G}^{(i)}} \alpha_{m,j}^{(i)} B_{m,j}^{(i)} + \sum_{k=1}^{n^{(i)}} \zeta_k^{(i)} Z_k^{(i)},$$

if there are any diagonal entries which are 0, set all entries in the corresponding row and column to be 0. Use the resulting linear equations to reduce the problem, and delete the 0 row and column from L_i . Also delete the entry in M_i with the same index as the deleted row and column. Repeat this step until there are no diagonal entries in L_i equal to 0.

- (g) If we eventually get $L_i = 0$, stop and output that there is no nonzero sum of squares.
- (h) Solve the linear matrix inequality

$$L_i(\alpha^{(i)}, \beta^{(i)}) \succeq 0$$

to see if there is a nonzero solution $(\alpha^{(i)}, \beta^{(i)})$.

- (i) If there is not, stop and output that there is no nonzero sum of squares.
- (ii) Otherwise, output the vector of polynomials

$$\sqrt{L(\alpha^{(i)}, \beta^{(i)})} M_i.$$

- (7) If there is no nonzero sum of squares, stop and output $\mathcal{G}^{(i)}$.
- (8) Otherwise, let $\phi_1, \dots, \phi_{r_i}$ be the entries of the outputted vector of polynomials. Compute a reduced left Gröbner basis for the

set $\mathcal{G}^{(i)} \cup \{\phi_1, \dots, \phi_{r_i}\}$ and let $\mathcal{G}^{(i+1)}$ be the resulting set. Go to (4).

9.1.1. *Properties of the Real Radical Algorithm.* We now prove Theorem 1.4, which presents some appealing properties of the Real Algorithm presented in §9.1.

Proof of Theorem 1.4. First, if $\deg(\iota_1), \dots, \deg(\iota_\mu) \leq d$, since we are using a degree lexicographic order to compute the reduced left Gröbner basis, it is clear from the left Gröbner basis algorithm that the outputted left Gröbner basis also consists of polynomials with degree bounded by d . Next, for the set $\mathfrak{C}^{(i)}$, if $\mathcal{G}^{(i)}$ consists of polynomials of degree bounded by d , then the only monomials which properly divide a monomial of degree bounded by d on the right must have degree less than d . Therefore the set $\mathfrak{C}^{(i)}$ has monomials of length at most $d - 1$. In particular, at each iteration, $\mathcal{G}^{(i+1)}$ is a reduced left Gröbner basis generated by $\mathcal{G}^{(i)}$, which has polynomials of degree bounded by d , and some polynomials in the span of $\mathfrak{C}^{(i)}$. Therefore, at each step, $\mathcal{G}^{(i)}$ always consists of polynomials of degree bounded by d . Finally, the polynomial (9.1) is a sum of polynomials with degree bounded by $2d - 1$. This all verifies the degree bounds in (1).

Second, at each step we are adding polynomials in the span of $\mathfrak{C}^{(i)}$ to $\mathcal{G}^{(i)}$ and then computing a reduced left Gröbner basis. Further, each monomial in $\mathfrak{C}^{(i)}$ is not divisible on the right by the leading monomial of an element of $\mathcal{G}^{(i)}$, so $\text{Span}(\mathfrak{C}^{(i)}) \cap \mathbb{R}\langle x, x^* \rangle \mathcal{G}^{(i)} = \{0\}$. Therefore the left module generated by $\mathcal{G}^{(i+1)}$ must properly contain the left module generated by $\mathcal{G}^{(i)}$. Since $\mathbb{R}^{1 \times \ell} \langle x, x^* \rangle_d$ is finite dimensional, this process must stop eventually. This proves (2).

Finally, at each step, consider finding a nonzero sum of squares of the form (9.1). Assume inductively that each $\mathcal{G}^{(i)} \subseteq \sqrt[r]{I}$. This is true at the outset since $\mathcal{G}^{(0)} \subseteq I \subseteq \sqrt[r]{I}$. If the SOS algorithm finds such a sum of squares, then it is equal to

$$\begin{aligned} M_i^* L_i(\alpha, \beta) M_i &= \left(\sqrt{L_i(\alpha, \beta)} M_i \right)^* \left(\sqrt{L_i(\alpha, \beta)} M_i \right) \\ &\in \mathbb{R}^{\ell \times 1} \sqrt[r]{I} + \sqrt[r]{I}^* \mathbb{R}^{1 \times \ell}. \end{aligned}$$

This implies that the outputted vector of polynomials from the real radical algorithm are polynomials in $\sqrt[r]{I}$, which gives $\mathcal{G}^{(i+1)} \subseteq \sqrt[r]{I}$.

If the SOS Algorithm outputs that there is no sum of squares, by Proposition 8.3, $(\mathcal{G}^{(i)}, \emptyset)$ is a \mathfrak{C} -basis, so by Theorem 7.3, this is enough to show that the left module generated by $\mathcal{G}^{(i)}$ is real. Since $\mathcal{G}^{(i)} \subseteq \sqrt[r]{I}$, this implies that $\mathcal{G}^{(i)}$ is a reduced left Gröbner basis for $\sqrt[r]{I}$. \square

10. ACKNOWLEDGMENTS

Author was partly supported by J.W. Helton's National Science Foundation grant DMS 1201498. Thanks to J.W. Helton and Igor Klep for their comments and advice.

REFERENCES

- [1] J. Bochnak, M. Coste, M.-F. Roy. Real Algebraic Geometry, volume 95. Springer Berlin, 1998.
- [2] K. Cafuta, I. Klep, J. Povh: NCSOSTools: a computer algebra system for symbolic and numerical computation with noncommutative polynomials, Optim. Methods Softw. **26** (2011) 363–380. Available from <http://ncsostools.fis.unm.si>
- [3] J. Cimprič, A Real Nullstellensatz for Free Modules, *preprint*, arXiv:1302.2358.
- [4] J. Cimprič, J. W. Helton, I. Klep, S. McCullough, C. S. Nelson, On real one-sided ideals in a free algebra, *preprint*, <http://arxiv.org/abs/1208.4837v1>. 1–32.
- [5] J. Cimprič, J.W. Helton, S. McCullough, C. S. Nelson, A non-commutative real Nullstellensatz corresponds to a non-commutative real ideal; algorithms, to appear in the Proc. Lond. Math. Soc., <http://arxiv.org/abs/1105.4150>, 1–35.
- [6] Cohn, P. M. Free ideal rings and localization in general rings. New Mathematical Monographs, 3. Cambridge University Press, Cambridge, 2006.
- [7] R. Curto, L. Fialkow: Solution of the truncated complex moment problem for flat data, Mem. Amer. Math. Soc. **119** (1996).
- [8] R. Curto, L. Fialkow: Flat extensions of positive moment matrices: Recursively generated relations, Mem. Amer. Math. Soc. **136** (1998).
- [9] D. W. Dubois, A nullstellensatz for ordered fields, Ark. Mat. **8** (1969), 111–114.
- [10] Goodearl, K. R. Ring theory. Nonsingular rings and modules. Pure and Applied Mathematics, No. 33. Marcel Dekker, Inc., New York-Basel, 1976. viii+206 pp.
- [11] E. Green, Multiplicative bases, Gröbner bases and right Gröbner bases, J. Symbolic Computations **29** (2000), 601–623.
- [12] J. W. Helton, I. Klep, and S. McCullough, The convex Positivstellensatz in a free algebra, Adv. Math. **231** (2012), pp. 516–534
- [13] J. W. Helton, I. Klep, and C. Nelson, A Perfect Positivstellensatz in a Free $*$ -Algebra, *in preparation*.
- [14] J. W. Helton and S. McCullough, A Positivstellensatz for Noncommutative Polynomials, Trans AMS, **356** (9) (2004), pp. 3721–3737
- [15] J. W. Helton and S. McCullough, Every convex free basic semi-algebraic set has an LMI representation. Annals of Mathematics **176** (2012), pp. 979–1013.
- [16] J.W. Helton, S. McCullough, M. Putinar: Strong majorization in a free $*$ -algebra, Math. Z. **255** (2007) 579–596.
- [17] J.W. Helton, M.C. de Oliveira, M. Stankus, R.L. Miller: NCAIgebra, 2012 release edition. Available from <http://math.ucsd.edu/~ncalg>
- [18] I. Klep and J. Povh, Semidefinite programming and sums of hermitian squares of noncommutative polynomials, J. Pure Appl. Algebra, **214** (2010), pp. 740–749.
- [19] I. Klep, M. Schweighofer, An exact duality theory for semidefinite programming based on sums of squares. To appear in Math. Oper. Res., arXiv:1207.1691.

- [20] J.-L. Krivine, Anneaux préordonnés. J. Analyse Math. **12** (1964), pp. 307–326.
- [21] J.-L. Krivine, Quelques propriétés des préordres dans les anneaux commutatifs unitaires. C. R. Acad. Sci. Paris, **258** (1964), 3417–3418.
- [22] Lam, T. Y. A first course in noncommutative rings. Second edition. Graduate Texts in Mathematics, 131. Springer-Verlag, New York, 2001. xx+385 pp.
- [23] Lam, T. Y. Lectures on modules and rings. Graduate Texts in Mathematics, 189. Springer-Verlag, New York, 1999. xxiv+557
- [24] M. Marshall, *-orderings on a ring with involution, Comm. Algebra **28** (3) (2000), pp. 1157–1173.
- [25] M. Marshall, *-Ordering and *-valuations on algebras of finite Gelfand-Kirillov dimension. J. Pure Appl. Algebra, **179** (3) (2003), pp. 255–271.
- [26] M. Marshall, Positive polynomials and sums of squares. Mathematical Surveys and Monographs, 146. American Mathematical Society, Providence, RI, 2008.
- [27] M. Putinar, Positive polynomials on compact semi-algebraic sets. Indiana Univ. Math. J. **42** (1993), 969–984.
- [28] J.-J. Risler, Une caractérisation des idéaux des variétés algébriques réelles. C. R. Acad. Sci. Paris, série A, **271** (1970), 1171–1173.
- [29] C. Scheiderer, Positivity and sums of squares: A guide to recent results. In *Emerging applications of algebraic geometry*, ed. by M. Putinar and S. Sullivan, IMA Vol. Math. Appl. 149, Springer-Verlag, New York 2009, 271–324. Zbl 1156.14328 MR 2500469 MR2500469 (2010h:14092)
- [30] K. Schmüdgen, Noncommutative real algebraic geometry—some basic concepts and first ideas. *Emerging applications of algebraic geometry*, 325–350, IMA Vol. Math. Appl., 149, Springer, New York, 2009.

CONTENTS

1. Introduction	2
1.1. Notation	2
1.2. Commutative Inspiration	3
1.3. Non-Commutative Polynomials	3
1.4. Left $\mathbb{R}\langle x, x^* \rangle$ -Modules	5
1.5. Main Results	7
1.6. Reader's Guide	8
2. Right Chip Spaces and Factorization of Monomials	8
2.1. Constant Matrices in the Complement of a Full Right Chip Space	9
2.2. Unique Factorization of Monomials	10
3. \mathfrak{C} -Orders and \mathfrak{C} -Bases	12
3.1. \mathfrak{C} -Bases	14
4. Double \mathfrak{C} -Orders	15
5. Positive Linear Functionals on $\mathbb{R}^{\ell \times \ell} \langle x, x^* \rangle$	18
5.1. The GNS Construction	22
5.2. Non-Commutative Hankel Matrices	23
5.3. The Matrix Non-Commutative Left Nullstellensatz	27
6. Extension to \mathbb{C} and \mathbb{H}	27
6.1. Quaternion Case	28
6.2. Extension of the Left Nullstellensatz to \mathbb{C} and \mathbb{H}	29
7. The Real Radical of a Left Module in $\mathbb{R}^{1 \times \ell} \langle x, x^* \rangle$	30
8. Left Gröbner Bases	33
8.1. Algorithm for Computing Reduced Left Gröbner Bases	35
8.2. Reduced Left Gröbner Bases are \mathfrak{C} -Bases	35
9. The Real Radical Algorithm	36
9.1. The Real Radical Algorithm	36
10. Acknowledgments	39
References	40